iX

MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

6 Juni 2008 € 5,50 H 10554

IT-Security:
Google findet Schwachstellen
VoIP-Sicherheit

1 × Microsoft, 5 × Linux:

Small Business Server

Vergleichstest, Sicherheitscheck

Neues Tutorial:
Ruby on Rails
Erste Schritte

Wahrheit und Wunschdenken:
RFID in der Praxis

Interaktives Web:
Actionscript-Tools

Embedded Systems:
Industrie-PCs

Parallelprogrammierung:
Erlang/OTP

Was der Aufschwung brachte:
IT-Gehälter 2008

Kommunikation statt Konfiguration:
Mail-Appliances

Server-Farmen:
Power6-Blades mit AIX 6.1 und SLES 10



Kommerzielle Xen-Virtualisierer:
Citrix XenServer vs. Virtual Iron

Juni 2008 www.ix.de
iX Magazin für professionelle Informationstechnik
Österreich € 6,20 Schweiz CHF 10,70 Benelux € 6,70 Italien € 6,70
Heise
4 199148 505501 06

Die Komplexitätsfalle

Wer in der IT-Welt zu Hause ist, weiß, dass sich sein Beschäftigungsfeld nicht gerade durch besondere Übersichtlichkeit auszeichnet. Zahllose sogenannte Standards, Frameworks, Vorgehensweisen und Architekturkonzepte beispielsweise in der Enterprise-Java-Disziplin sollen dem Entwickler zwar eigentlich die Arbeit erleichtern, steigern aber allein durch ihre schiere Menge die Verwirrung. Und einige als Revolutionen angekündigte Erscheinungen wie Enterprise Java Beans gelten unter Kennern sogar als mittlere Katastrophe. Jede Release verspricht, einfacher zu sein als die letzte, kann sich mit ihrem Vorgänger jedoch nicht mehr unterhalten. Für den Unbedarften riecht das Ganze nach dem Spaghetti-Code von morgen.

Auffällig häufig benutzen Keynote-Redner, Referenten und Autoren den Terminus „Problem“. Knifflige Aufgaben gibt es in der Systementwicklung tatsächlich zuhauf: Komplexität entsteht nicht nur durch neue Anforderungen, sondern auch durch die rasant steigende Anzahl von Beziehungen zwischen den beteiligten Menschen und Maschinen. Zusätzliche Schwierigkeiten verursacht der Effekt der Emergenz: Mannigfaltig gekoppelte natürliche oder künstliche Systeme entwickeln regelmäßig neue und nicht vorhersehbare Eigenschaften.

Trotz der in den letzten Jahren enorm verfeinerten Werkzeuge und Techniken verhalten sich etwa Enterprise-Anwendungen immer noch ziemlich dumm. Der Aufwand steht hier oft in keinem gesunden Verhältnis zum Ergebnis. Frustrierte Anwender, hoher Schulungsaufwand, Inkonsistenzen, wucherndes Schnittstellengestrüpp, Altlasten, Bürokratie – alles wie gehabt. IT und Geschäft fremdeln immer noch, obwohl Hersteller von Werkzeugen für das Managen von Geschäftsprozessen gern darauf hinweisen, dass sogar der Anwender aus der Fachabteilung ihre Produkte bedienen können soll.

Der IT-Markt scheint nicht nach drögen kaufmännischen Regeln zu ticken, sondern orientiert sich eher an irrationalen Veranstaltungen wie dem Pop-Business. Skurrile, manchmal quasireligiöse Berufsbezeichnungen deuten darauf hin, dass hier nicht der nüchterne Techniker die Szene beherrscht. Die Java-Gurus, BPM-Päpste und Open-Source-Evangelisten haben klar die Deutungshoheit.

Prof. Nikolaus Wulff von der FH Münster lieferte auf der diesjährigen JAX („Die Grenzen der Komplexität“) zwar auch keine Lösung, aber zumindest eine Erklärung für das Dilemma. In allen Systemen gibt es Phasen des Übergangs, geprägt von Instabilität, Chaos und evolutionären Sackgassen. All diese Systeme streben jedoch eifrig danach, wieder ein stabiles Gleichgewicht zu erreichen. Insgesamt ist der Druck im Kessel enorm hoch, die Grenzen der Skalierbarkeit sind bald erreicht. Fundamentale Änderungen erwartet Wulff allerdings erst in den nächsten 10 bis 15 Jahren. Etwas Dampf entweicht zurzeit nur über Ausweichstrategien wie schnellere Rechner, Grid Computing und Virtualisierung.

Miko Matsumura, Vice President und Deputy CTO (sic!) der Software AG schlug auf derselben Veranstaltung vor, aus Gründen der Komplexitätsreduzierung alle Beziehungen zwischen Maschinen und Menschen in einem Repository auszulagern. Zufällig verkauft sein Arbeitgeber dafür ein geeignetes Werkzeug. Ansonsten solle man sich auf gemeinsame Standards und Vorgehensweisen einigen („let’s agree“, hat nachweislich noch nie richtig funktioniert). Dafür bietet die IT-Industrie selbstverständlich die notwendigen Softwareprodukte. Die firmieren unter den Begriffen Governance und Compliance und sollen endlich für Ordnung sorgen. Aber auch dafür gibt es Tools, Standards und Frameworks. Und so bleibt die IT vorerst das, was sie schon immer war: Die größte Arbeitsbeschaffungsmaßnahme aller Zeiten.

Jürgen Diercks

JÜRGEN DIERCKS





Im wahrsten Sinne des Wortes „wie auf Schienen" soll die Entwicklung einer Webabwendung mit dem Framework Ruby on Rails laufen. Im ersten Teil des Tutorials geht es um die dennoch nötigen initialen Tätigkeiten.

Seite 124

Virtualisierung: XenServer und Virtual Iron

Der unter anderem von der Bill-und-Melinda-Gates-Foundation unterstützte Open-Source-Virtualisierer Xen ist jetzt auch als Bestandteil von zwei kommerziellen Paketen erhältlich: XenServer und Virtual Iron.

Seite 67



Aufschwungserwartungen: IT-Gehälter 2008

Trotz vielfach beklagten Fachkräftemangels sind die Gehälter in der IT kaum gestiegen – die Gewerkschaften konstatieren sogar Einkommenseinbußen. Die Wahrheit erschließt sich wie so oft erst auf den zweiten Blick.

Seite 97



Linux vs. Microsoft: Small Business Server

Microsofts Small Business Server galt einmal als konkurrenzlos, wenn es um eine problemarme All-in-one-Lösung für kleine und mittlere Unternehmen ging. Doch mittlerweile ist im Linux-Lager Konkurrenz entstanden. Ob diese schon mithalten kann und ein schonungsloser Blick auf die Sicherheitslage auf den

Seiten 48 und 62



Marktübersicht: E-Mail-Appliances

Spam hin, Spam her – E-Mail bleibt der meistgenutzte Internetdienst. Gerade darum ist vielleicht das Aufsetzen eines eigenen Mailservers vielen Administratoren zu heikel, und sie greifen lieber auf vorkonfigurierte Appliances zurück.

Seite 89

Quelle gesucht

(Recht: Zurückholen ausgelagerter Dienstleistungen; *iX* 4/08; S. 126)

Ich genieße regelmäßig Lektüre nicht nur der *iX*-Redaktion, sondern aus dem ganzen Hause Heise. Sehr interessiert hat mich der Artikel „Alles auf Anfang“ von Herrn Meyer-Spasche, in dem es um das Backsourcing ausgelagerter Dienstleistungen geht. Erwähnt wird, dass nur 30 % der Outsourcing-Kunden zufrieden seien, was Statistiken belegen würden. Nur, welche Statistiken sind dies? Es ist leider keine Quelle angegeben. Ich finde überwiegend gegenteilige Aussagen.

TIMO ABEND, VIA E-MAIL

Im Wesentlichen bezog ich mich auf die folgenden Studien:
– „Sourcing-Studie 2007“ des Magazins CIO (zusammen mit TU München und Deloitte), die mir leider nur in Papierform (Heft 05/2007) vorliegt (einen Pressespiegel gibt es unter www.presseportal.de/pm/39396/980540/idg_cio_it_wirtschaftsmagazin);
– „Outsourcing Report 2008“ von Deloitte (Download unter www.deloitte.com/dtt/cda/doc/content/2008%20OSR%20-%20Why%20settle%20for%20less%281%29.pdf). Diese Studie muss man besonders sorgfältig lesen, denn sie suggeriert zu Beginn gerade 70 % Zufriedenheit – weist dann aber selbst auf den Widerspruch zu den sonstigen Ergebnissen hin.
– TPI Outsourcing Analyse 2007, in Kurzform verfügbar unter www.tpi.net/pdf/researchreports/Restructuring_ResearchReport%20Jan_24_07.pdf
(Georg Meyer-Spasche)



Enttäuschend

(Interaktives Web: Software für Onlineforen; *iX* 5/08; S. 38)

Sehr hatte ich mich auf einen Artikel zum Thema Forensoftware gefreut. Allerdings machte die Vorfreude ausgewachsener Enttäuschung Platz, als ich den Artikel wirklich zu lesen bekam.

Wurde in der Einleitung ausgiebig auf die besonderen Sicherheitsprobleme von Forensoftware hingewiesen, wurde in der eigentlichen Gegenüberstellung nicht auf die Abwehrstrategien eingegangen. Gerade ein solcher Blick „unter die Haube“ wäre eine interessante Vergleichsachse gewesen, die über die Informationen auf den Herstellerhomepages hinausgegangen wäre. Gerade auf die „wunden Punkte“ wie die Abwehr von Mime-Sniffing XSS in Dateiuploads hätte man eingehen müssen.

Ähnliches könnte man über die Möglichkeiten der Anbindung an bestehende Anwendungen sagen. Auch Hinweise auf strategische Partnerschaften, wie etwa zwischen phpBB und Joomla! wären für manche Leser wissenswert gewesen.

Auch wurde oft der Eindruck von Alleinstellungsmerkmalen erweckt, etwa

DER DIREKTE DRAHT ZU iX

Redaktion iX
Postfach 61 04 07
30604 Hannover

Fax: 05 11/53 52-361
E-Mail: <user>@ix.de
Web: www.ix.de

Direktwahl zur Redaktion: 05 11/53 52-387

Für telefonische Anfragen zu Artikeln, technischen Problemen, Produkten et cetera steht die Redaktion wie gewohnt während der Lesersprechstunde zur Verfügung. Und zwar:

Montag bis Freitag, 11 bis 12 Uhr

Bitte nur während der genannten Zeiten anrufen und möglichst die angegebene Durchwahl benutzen.

<Durchwahl>	<user>	
-387	post	Redaktion allgemein
-377	avr	(André von Raison)
-590	ck	(Christian Kirsch)
-387	cle	(Carmen Lehmann)
-374	hb	(Henning Behme)
-379	jd	(Jürgen Diercks)
-386	js	(Jürgen Seeger)
-367	ka	(Kersten Auel)
-153	mm	(Michael Mentzel)
-787	mr	(Michael Riepe)
-373	rh	(Ralph Hülsenbusch)
-689	sun	(Susanne Nolte)
-368	un	(Bert Ungerer)
-535	ur	(Ute Roos)
-384	wm	(Wolfgang Möhle)

Listing-Service:
Sämtliche in iX seit 1990 veröffentlichten Listings sind über den iX-FTP-Server erhältlich:
ftp.heise.de/pub/ix/

iX-Link Bei Artikeln mit diesem Hinweis können Sie auf www.ix.de das zugehörige Argument (ixJJMMSSS) eingeben, um eine klickbare Liste aller URLs zu bekommen.

der Hinweis auf die Tabellenlosigkeit des Burning Boards – z. B. ist auch das phpBB tabellenfrei bzw. verwendet Tabellen semantisch korrekt. Schließlich – ich gebe zu, keineswegs neutral in diesen Fragen zu sein – war der wertende Hinweis auf RSS und dessen Abwesenheit bei phpBB fragwürdig. Zum einen gibt es phpBB Module für RSS, zum anderen ist ein Pull-Medium für Foren mit ACL schlecht geeignet. Daher setzt phpBB auf Push mit Jabber und E-Mail.

Jedenfalls wären harte Benchmarks sehr erfreulich gewesen.

Nichtsdestotrotz: danke für die Übersicht – Foren sind neben Blogs ein sehr häufiger Wunsch für Homepages. Etwas neutrale Information tat Not.

HENRY SUDHOF, BERLIN

Gewaltige Mängel

(Interaktives Web: Software für Onlineforen; *iX* 5/08; S. 38)

Ich möchte sie darauf hinweisen, dass Ihr aktueller Leitartikel für Forensoftware gewaltige Mängel enthält.

1. ist das wBB3.0 im Sommer 2007 erschienen.
2. beherrscht das wBB3.0 eigene BBCodes, diese können über das ACP angelegt werden.
3. sollten Sie ihre Quellen genauer prüfen und eventuell die Forensoftware kaufen und selbst testen und sich nicht nur auf dritte Quellen verlassen.

KARSTEN ACHTERRATH,
VIA E-MAIL

Kleiner Fauxpas

(Embedded Systems: Entwicklung mit dem iPhone SDK; *iX* 5/08; S. 131)

Vielen Dank für den Artikel, der einen schnellen Überblick zur iPhone-Entwicklung schafft. Auf einen kleinen Fauxpas muss ich Sie aber hinweisen:

Objective-C kennt keine Methoden, die runde Klammern benutzen.

Im Artikel besprechen Sie Methoden, die *applicationDidFinishLaunching()* und *addSubview()* heißen sollen. Tatsächlich sind die Namen aber *applicationDidFinishLaunching:* und *addSubview:*.

Die Wichtigkeit der Unterscheidung wird an zwei Beispielen klar.

1. Methoden mit mehreren Argumenten: In Java wird *setObjectForKey (Object anObject, String aKey)* zu *setObjectForKey()*.

In ObjC wird *setObject:(Object)anObject forKey:(NSString)aKey* zu *setObject:forKey:*.

2. Dynamische Methodenaufrufe: *@selector(addSubview())* ist ein Syntax-Error. *@selector(addSubview:)* ist richtig.

ALEXANDER SPOHR,
VIA E-MAIL

Windows 2008 und Samba

(Samba-Tutorial III: Samba als primärer Domänencontroller; *iX* 5/08; S. 140)

Ist es möglich, mit Ihrem Tutorial einen Samba-Server 3.0.28 als Domänenmitglied in eine Windows-Server-2008-Domäne einzubinden ?

ANDREAS KUCZERA, MAINZ

Nein, leider bringt Windows 2008 einige Änderungen in den Sicherheitspolicies und im Kerberos mit sich, die die 3.0.28 noch nicht beherrscht. Selbst die 3.0.28a hat da noch Probleme. Mit den aktuellen Patches, die zur 3.0.28b führen werden, geht es aber.
(Volker Lendecke)

Ergänzungen und Berichtigungen

(Systeme: Aus System p und i wird Power Systems; *iX* 5/08; S. 18)

Nicht im wassergekühlten Power 575, sondern im Power 595 laufen die Power6-Prozessoren mit 5 GHz. Der Power 575 arbeitet mit 4,7 GHz.

(Vorschau: OS-Business-Modelle/ECM als Open Source; *iX* 5/08; S. 162)

Aus redaktionellen Gründen mussten leider die beiden angekündigten Artikel in eine spätere Ausgabe verschoben werden.

Die *iX*-Redaktion behält sich Kürzungen und auszugsweise Wiedergabe der Leserbriefe vor. Die abgedruckten Zuschriften geben ausschließlich die Meinung des Einsenders wieder, nicht die der Redaktion.



Neue Schwerpunkte der Hannover Messe: Robotik und Forschung

Weltweiter Kick-off

Christopher Kunz

Fußballspielende Roboter und kuschelnde Elektrorobben tummelten sich auf der diesjährigen Hannover Messe. Die konnte mit rund 200 000 Besuchern den 2006 befürchteten Abwärtstrend stoppen.

Die Talsohle scheint durchschritten – im Vergleich zum schwach besuchten Vergleichsjahr 2006 kamen mit 200 000 Interessenten satte 30 Prozent mehr zur weltgrößten Industriemesse in Hannover. Obwohl man damit die 230 000 aus 2007 deutlich verfehlte, zogen die Organisatoren auf ihrer abschließenden Pressekonferenz ein positives Fazit: „Die Hannover Messe fasziniert wieder Menschen“, so Sepp D. Heckmann, der Vorstandsvorsitzende der Messe AG. Der für die Aussteller bedeutsame Fachbesucheranteil sei um rund 25, der der Entscheider um etwa 20 Prozent gestiegen – nach den während der Messe durchgeführten Umfragen waren also knapp 180 000 Besucher vom Fach und 127 000 besuchten die Messe mit Entscheidungsbefugnis.

Gemeinsam gegen die Tücken der Technik

Besonders gut ließ sich die von Heckmann festgestellte Faszination in den diesjährigen Schwerpunktthemen Robotik und Forschung feststellen – es kreuchte und fleuchte allerorten und bisweilen kam der neugierige Besucher sich vor wie in einer Fantasiewelt aus George Lucas’ Feder.

Augenfällig war die Anziehungskraft der verspielten elektronischen Zeitgenossen in Halle 25, dem Austragungsort der RoboCup German Open. In mehreren Disziplinen und Ligen kämpften Roboter gegeneinander und ihre Besitzer häufig gegen die Tücken der Technik. Noch kurz vor dem Eröffnungsmatch dominierten hektische Umbau- und Fehlersucharbeiten die Spielfelder, bevor sich die Roboter im klassischen Roboterfußball, dem Hindernisparcours der „RoboCup Rescue“-Liga oder einem Wettbewerb für Serviceroboter – Web-2.0-tauglich „RoboCup@ Home“ genannt – messen konnten. Neben vielen europäischen Ländern war der Iran mit drei Mannschaften vertreten – die Teams aus Teheran und Dezfoul nahmen an den via Internet ausgetragenen Wettbewerben zur Robotersimulation teil.

In der wie in den vergangenen Jahren für Aussteller aus Forschung und Wissenschaft reservierten Halle 2 kamen Science-Fiction-Fans abermals auf ihre Kosten. Japan, das Partnerland der HMI 2008, zeigte Vergangenheit, Gegenwart und Zukunft der Robotik mit so unterschiedlichen Exponaten wie antiken Miniatur-Bogenschützen, anmutigen Mannequin-Robotern und einem tanzenden Humanoiden. Direkt daneben präsentierte das AIST, eines der größten Forschungsinstitute Japans, aktuelle Entwicklungen von der Nanotechnologie bis zur Robotik.

Zu den meistfotografierten Ausstellungsstücken dürfte PARO, eine plüschige Babyrobbe, zählen. Ähnlich wie bereits im Spielzeughandel erhältliche Artgenossen reagiert dieser Roboter auf seine Umwelt, kann Verhaltensweisen erlernen und Kontakte mit menschlichen Bezugspersonen pflegen. Die Elektrorobbe wird in Japan seit drei Jahren in der Kinder- und Senioren-Therapie eingesetzt, um Einsamkeit und emotionalem Stress entgegenzuwirken. Paro-Erfinder Takanori Shibata kündigte an, das Produkt „noch in diesem Jahr“ auch nach Europa und die USA zu exportieren.

Deutlich handfester ging es bei den Exponaten zur autonomen Fahrzeugnavigation zu. Gleich mehrere Forschungseinrichtungen, darunter das Fraunhofer-Institut AIS und die TU Braunschweig, präsentierten Autos, die an der 2007 letztmalig durch das US-Verteidigungsministerium ausgerichteten „DARPA Urban Challenge“ teilgenommen haben. Bei diesem Wettbewerb geht es darum, das Auto ohne Fahrer oder Fernbedienung über eine Hindernisstrecke auf einem Kasernengelände zu bewegen, anderen Autos auszuweichen und sich möglichst fehlerfrei im Straßenverkehr zu bewegen. Diese Aufgabe stellt enorme technische Anforderungen an die Entwickler, die der Herausforderung auf unterschiedliche Weise begegneten. Der vom Fraunhofer IAIS entwickelte Wagen nutzt einen 3D-Laserscanner als wichtigste Schnittstelle zur Außenwelt, um Hindernisse, andere Wagen und die Straße zu erkennen. Dieser Laserscanner kann jedoch auch für andere Zwecke eingesetzt werden – etwa zur Planung von Schwerlasttransporten oder um die Sichtbarkeit und damit die Wirkung von Werbeplakaten zu testen.

Für Radfahrer präsentierte das Fraunhofer-Institut ein adaptronisches Pedal, das anhand eines eingegossenen Piezosensors messen kann, wie gleichmäßig der Fahrer tritt, und das diese Daten per Funk in Echtzeit übermittelt. Das Pedal entstand als Demonstration des Projektes InGus, das Gussteilen aus Leichtmetall ein elektronisches Innenleben verleihen soll. Dessen eigentliches Ziel ist übrigens ein ganz anderes: Man will per RFID Raubkopien von Autoteilen ermitteln.



Der humanoide Roboter HRP-2 kann sogar tanzen.

Ergonomische Fabriken durch AR

Fabrikplanung – ein klassisches Thema der Hannover Messe – steht im Mittelpunkt eines Exponats des Fraunhofer-Instituts IAO. Das Projekt „iTeach“ bietet dem Planer die Möglichkeit, mithilfe menschlicher Modelle in einer dreidimensionalen Umgebung Abläufe und Arbeitsstationen zu optimieren. Die Menschmodelle können typische Bewegungsabläufe simulieren und ergonomische Herausforderungen wie schmerzhafte oder rückenschädigende Haltungen deutlich machen.



Auch die Firma Metaio setzt auf „Augmented Reality“ in der Planung von Fabrik- und Montagehallen: Anhand eines Markers, der auf den Hallenboden gelegt und fotografiert wird, berechnet die Software die korrekte Perspektive, und Maschinen, Roboter oder Polstermöbel lassen sich perspektivisch korrekt direkt in der fotografierten Umgebung platzieren. Bei der Planung neuer Produktionsstraßen in bestehenden Gebäuden kann man so eventuelle Hindernisse bereits im Frühstadium identifizieren – insbesondere im Fahrzeugbau können die Planer auf diese Weise teure Fehler vermeiden.

Blackberry steuert

Der Schadensbegrenzung in der Produktion dient auch Extend 7000 der Schad GmbH. Dieses Softwaresystem informiert die Techniker nicht nur über Fehler, sie können auch mit ihrem Blackberry-Handheld in die Maschinensteuerung eingreifen. Die Software unterstützt auf der Anlagenseite die weit verbreiteten Simatic-Steuerungen von Siemens. Der Java-Client greift auf die Infrastruktur von Research in Motion zurück, die Daten gelangen über das Mobilfunknetz zu der mit dem Internet verbundenen Maschine.

Das Projekt „Bingo Voting“ vom europäischen Institut für Systemsicherheit der Uni Karlsruhe hingegen befasste sich mit einem eher HMI-untypischen Thema – der Verifizierbarkeit von Wahlverfahren. Basierend auf einem Zufallsgenerator und einem komplexen Sicherheitsprotokoll haben die Karlsruher eine Methode entwickelt, die jedem Wähler erlaubt, die ordnungsgemäße Auszählung seiner Stimme zu überprüfen. Das verhindert Wahlmanipulation und stärkt das Demokratievertrauen.

Interessierte Jugendliche konnten sich bei der Nachwuchsinitiative „TectoYou“ über ihre Chancen in der Industrie informieren. Geführte Touren über die Messe und Angebote zum Mitmachen sollten das Interesse an technischen Berufen wecken – mehr als 20 000 junge Menschen, darunter viele Schulklassen, folgten dem Angebot. (ka)

Open Source meets Industry

Linux steuert Maschinen

Barbara Lange

Linux läuft verstärkt auch im industriellen Umfeld. „Open Source meets Industry“ – so das Motto der eintägigen Sonderveranstaltung auf der Hannover Messe.



Wenn Open-Source-Software einen Laserstrahl steuert, treffen zwei Welten aufeinander. Fünf bekannte Linux-Kernel-Entwickler berichteten den 150 Vertretern von Automatisierungsindustrie und Maschinenbau von ihrer Arbeit am Linux-Kernel und stellten dar, was Linux überhaupt ist. Veranstalter waren der Verband Deutscher Maschinen- und Anlagenbau VDMA, die Deutsche Messe AG und das Open Source Automation Development Lab OSADL – eine eingetragene Genossenschaft, die Open-Source-Software in besagten Industriezweigen fördert und koordiniert (www.osadl.org). Zu den 21 Mitgliedsunternehmen zählen die Eltec Elektronik AG, Homag Holzbearbeitungssysteme AG, Trumpf GmbH + Co. KG und Linutronix GmbH.

Das Programm war auf die Einsteiger aus der Industrie ausgerichtet. So berichtete Linux-Kernel-Entwickler Alan Cox aus dem Geschichtsbuch des freien Betriebssystems, Rechtsanwalt Till Jaeger erklärte die aus der Nutzung von Open Source resultierenden Rechte und Pflichten der Lizenzierung.

Bessere Ergebnisse durch Open Source

Andrew Morton erläuterte die Arbeitsweise der Linux-Community und den Aufbau von Linux. Vor allem die kooperative Arbeitsweise zeichne Open-Source-Software aus und führe immer zu besseren Ergebnissen. Umsonst wie zu den Pionierzeiten arbeiten dabei nur noch wenige: Nach einer Studie der Linux-Foundation erhalten mittlerweile lediglich 13,9 Prozent der Linux-Entwickler kein Geld von der Industrie, vor allem als Tester, wie Linux-Entwickler Greg Kroah-Hartmann berichtete. Er forderte die Industrie auf, ihnen ihre Treiber-Anforderungen zu schicken, die sie dann unentgeltlich realisieren würden. Auch Treiber von selten eingesetzter Hardware sollen Bestandteil des Kernels werden.

In der Industrie angekommen

Nach der Einschätzung von Carsten Emde, Geschäftsführer von OSADL, ist Open Source mit dieser Veranstaltung und dem Messestand „Application Parc“ bei der Industrie angekommen. Klar wurde, dass die Entwickler ernsthaft an den besonderen Anforderungen arbeiten, die die Industrie an offene Betriebssysteme stellt. Dazu gehören die Echtzeitfähigkeit und die Virtualisierung auf Kernel-Ebene. Beides ist so gut wie realisiert, führte Emde aus. Seit Ende 2007 seien große Teile des „Real time Preemption Patch“ in den Linux-Kernel 2.6.24. integriert worden.

Für Industrieunternehmen, die den Einsatz von Linux erwägen, lieferte Open-Source-„Evangelist“ Bruce Perens eine interessante Entscheidungshilfe. Er unterschied zwischen „differenzierender und nicht-differenzierender Software“: Erstere macht das besondere Know-how von Unternehmen aus und sollte geschlossen bleiben. Dieser Anteil beträgt aber nur fünf Prozent, so Perens. Die überaus deutliche Mehrheit von 95 Prozent aller Unternehmenssoftware sei für alle Unternehmen nützlich und damit nicht differenzierend. Dieser Anteil könne nur Open Source sein. (ka)


Quelle: OSADL, Fotograf Klaus Fricke

Geschichtsstunde mit Linux-Kernel-Entwickler Alan Cox



Robuste Tragbare

Der Wunsch nach mobilen PCs für den Außeneinsatz steigt. Kontron (http://de.kontron.com/NotePac/) stellte das rugged Notebook NotePAC Ultra-M230N und das Tablet E100 vor, beide erfüllen die Norm IP54 (Spritzwasserschutz). Das M230N erfüllt zudem Mil-STD-461 und verträgt Stürze aus 90 cm Höhe. Zur Ausrüstung gehört ein 14,1"-XGA- oder ein 15,1"-'SXGA-Bildschirm sowie maximal 4 GByte RAM, eine 1,5-GHz–Core2-Duo-CPU und eine 2,5"-Festplatte mit 250 GByte Kapazität.

Das Tablet E100 erfüllt Mil-STD-810F und darf aus 1,2 m Höhe auf Beton stürzen. Die Auflösung des 8,4"-SVGA-Displays beträgt 800 × 600 Pixel. Beim 800-MHz-Pentium-M handelt es sich um einen Ultra Mobil Coremit bis zu fünf Stunden Akkulaufzeit. Der Speicherausbau endet bei 1 GByte. Bei der 80-GByte-Festplatte setzt der Hersteller auf das besonders stoßunempfindliche 1,8"-Format.

Als Schnittstellen stehen USB 2.0, Cardbus, 1-GBit-LAN sowie Audio bereit. Gemeinsam sind dem E100 und dem M230N die Schnittstellen von USB bis LAN sowie UMTS (HSDPA), WLAN, Bluetooth und GSM. Die Dockingstations sind für den Einbau im Fahrzeug gedacht. Das M230N verfügt zusätzlich über ein Modem und RS232, VGA, LPT sowie IRDA.

IPC2U (www.ipc2u.de) zeigte das Ruggedbook 800 von Rumoco. Es handelt sich um einen Tablet-PC mit 10,4"-Display (1024 × 768), dieser erfüllt die Normen MIL810F/461E und IP54. Der Temperaturbereich ist auf den Bereich von -20 bis +60 Grad Celsius erweitert. Die Akkulaufzeit beträgt bis zu sieben Stunden. IPC2U verwendet Intel-Prozessoren der Yonah-Familie. Es passen maximal 2 GByte DDRII-RAM in das Gerät, ein PCMCIA-Typ-II- und ein Compact-Flash-Typ-II-Slot dienen zur Erweiterung. Erwartungsgemäß verfügt auch dieses System über WLAN, Bluetooth, USB, RS232, GBit-LAN und Audio sowie ein Modem.

Brennstoffzelle als USV

Im Brennstoffzellenpark führte Rittal einen 5-kW-Generator vor. Er besteht aus einem 1,22 m hohen Schrank mit einer Standfläche von 85×85 cm, in dem sich die Brennstoffzelle mit Zubehör befindet, sowie einem Schrank für die Wasserstoffflaschen. Die Anlage liefert minimal 1 kW und verbraucht bei 3 kW 34 slqm (standard litre per minute) und 63 slqm bei 5 kW. Eine 50-l-Gasflasche reicht für 10 kWh. Die Anlage liefert 48 V Gleich- oder 230 V Wechselspannung.

Die Brennstoffzelle „verbrennt“ den Wasserstoff mithilfe des Luftsauerstoffes, der über einen Kompressor in die Zelle gelangt. Er ist die Ursache für die Schallemissionen von knapp 60 dB (in einem Meter Abstand). Wird der Schrank im Außenbereich aufgestellt, erhöht sich der Stand-by-Verbrauch von 200 auf 800 W, verantwortlich ist dafür eine Zusatzheizung für die Zelle. Die Wartung soll sich auf einen periodischen Luftfilterwechsel beschränken.

Compact PCI gut bestückt

Dass Compact PCI seinen Namen zu Recht trägt, zeigt die Firma EMTrust (www.emtrust.de) mit dem ICP-PM-8. Auf 100 × 160 mm befindet sich ein PC mit Pentium M760, bis zu einem Gigabyte DDR-RAM, ein CF-Sockel und eine 2,5"-IDE-Festplatte. Auf der zwei Einschübe breiten Frontplatte befinden sich zwei GBit-LAN-, eine VGA-, eine PS/2-, drei USB- und zwei serielle Schnittstellen (RS232/485). Bei der Grafik setzt der Hersteller auf eine ATI Radeon mit 32 MByte RAM, die eine maximale Auflösung von 2048 × 1536 Pixel liefert, sowie ein Panellink-Interface zum Anschluss von Monitoren mit DVI-Eingang. Zur Sicherheit tragen zwei Watchdogs bei.

Flacher Panel-PC

Der acht Höheneinheiten hohe IPPC-7157A Panel PC von Advantech (www.advantech.de) ist mit einem 15"-TFT Touchscreen lieferbar. Die Frontseite ist staub- und spritzwassergeschützt, die Einbautiefe beträgt nur 160 mm. Im PPC-7157A ist ein Industrie-ATX-Board verbaut, das einen PCIe-16-, einen PCIe-1- und fünf normale PCI-Steckplätze bietet. Es kommen Prozessoren mit dem Socket 775 vom Pentium 4, Celeron D bis zum Pentium D (Dual Core) mit bis zu 3,2 GHZ infrage. Der Speicherausbau endet bei 4 GByte (DDR2). Als Schnittstellen stehen 4 × USB 2.0, 2 × GBit-LAN, ein Parallelport und zwei serielle zur Verfügung. Bei einer der seriellen Schnittstellen kann man zwischen RS232, RS422 oder RS485 umschalten.

Bitkom: Gute Chancen im Embedded-Bereich

Embedded Systems sind zentraler Bestandteil aktueller Produkte der Investitionsgüter-Industrie. Ein Grund für Bitkom für ein Pressegespräch auf der Hannover Messe – gleichzeitig eine Premiere des ITK-Branchenverbands auf der traditionsgemäß für Maschinen und Anlagen bekannten Messe.

„Ob in der Medizintechnik, bei Herzschrittmachern und Magnetresonanztomographen oder der Automation von industriellen Anlagen, überall heißt es: Embedded Systems inside.“ Das betonte Bitkom-Vizepräsident Heinz-Paul Bonn. Die verarbeitende Industrie erziele rund 80 Prozent ihrer Wertschöpfung mit Produkten, die Embedded Systeme enthalten. So befinden sich in aktuellen Mittelklassewagen mittlerweile über 70 Prozessoren – vor 25 Jahren seien es erst sechs gewesen. In einem einzigen Auto laufen Softwarekomponenten mit 10 Millionen Codezeilen – 2015 sollen es 100 Millionen sein.

Genug zu tun also für Softwareentwickler. 80 000 Systementwickler arbeiten hierzulande an Embedded Software, berichtete Bonn. Weiterer Trend: Lange Jahre haben Anwenderbranchen wie die Auomobilindustrie oder der Maschinenbau ihre Embedded Software selbst entwickelt. Nun haben sich immer mehr neue Unternehmen auf die Embedded Systems spezialisiert und entwickeln zum Beispiel mit Embedded Linux oder Java Micro Edition.

Der Grad der Auslagerung der Softwareentwicklung für Embedded Systems ist je nach Region noch sehr unterschiedlich: In Europa lagern 34 Prozent aus, in den USA sind es 47 Prozent, in Japan 76 Prozent. Dieser Trend wird sich verstärken, so die Einschätzung.

Bislang steht Deutschland im internationalen Vergleich gut da. Nach den USA und Japan ist Deutschland derzeit der drittgrößte Hersteller. Aber aufgrund der Konkurrenz aus asiatischen Ländern wie Südkorea, China und Indien ist diese starke Stellung in Gefahr, warnt Bonn. Sein Verband rechnet für die asiatische Embedded-Systems-Industrie (ohne Japan) bis 2010 mit einem jährlichen Wachstum von 14 Prozent, für Europa sind es 8 Prozent. „Nur schnelles Handeln kann die bislang gute deutsche Marktposition erhalten“, betonte Bonn.

Aber die Bedeutung von Embedded Systems speziell für den Investitionsgüterbereich werde in Deutschland noch nicht richtig erkannt: Zum einen seien die Systeme unsichtbar. Zum anderen gäbe es keine eigenständige Embedded-Systems-Industrie, sondern die Systeme entstünden an der Schnittstelle zwischen Halbleiter- und Softwareindustrie auf der einen Seite und den Anwenderbranchen auf der anderen Seite.

Mit zwei Maßnahmen will Bitkom dem entgegenwirken: Bereits Ende letzten Jahres hat der Verband einen eigenen Arbeitskreis „Softwareintensive eingebettete Systeme“ gegründet. Dann wird es im Herbst eine neue Studie geben: Beauftragt wurden Pierre Audoin Consultants (PAC) und TechConsult. Beteiligt ist auch das Bundeswirtschaftsministerium für Wirtschaft und Technologie.

Barbara Lange

Business Integration Forum: Fortschritte bei SOA

Bunter Reigen

Achim Born

Wieder bot das Business Integration Forum in Wiesbaden reichlich Stoff zum Thema. Einige sehen hier Open-Source-Produkte im Aufwind, andere wollen die leidigen Integrationsaufgaben SaaS-Anbietern überlassen.

Wer sich heute über IT-Integration unterhält, kommt um die serviceorientierten Architekturen nicht herum. So war es konsequent, dass Wolfgang Martin zum Auftakt des diesjährigen Business Integration Forum über den Status Quo des marketingträchtigen Themas referierte. „Der Hype ist raus, die Einschätzung der Bedeutung von SOA ist realistischer geworden“, fasste der Vorsitzende des IIR-Kongresses in Wiesbaden die Ergebnisse des diesjährigen SOA-Checks zusammen.

Seinen Ausführungen zufolge haben die Firmen gegenüber 2007 nachweisbar Fortschritte gemacht. So sei im Zusammenhang mit SOA der Top-down-Ansatz mit Geschäftsprozessen als Ausgangspunkt akzeptiert. Allerdings belegten die Ergebnisse der Umfrage auch, dass der Zielerreichungsgrad der SOA-Projekte (siehe Abb. 1) nach wie vor zu wünschen übrig lässt. Dieses Ergebnis weist nach Ansicht von Martin auf eine mangelhaft ausgeprägte SOA-Governance in den Unternehmen hin. Das Management müsse deshalb dringend sein Verständnis für die administrativen und organisatorischen Aufgaben von Services und Prozessen verbessern, andernfalls drohe ein Servicechaos.

Services lassen sich in einer SOA auf allen Ebenen finden – von der Infrastruktur über fachliche Komponenten bis hin zu Analysediensten oder Dokumentenverarbeitung. Zudem werden Prozesse, Regeln und Stammdaten vermehrt applikationsunabhängig als Services bereitgestellt. Entsprechend bunt gestaltet sich der Reigen der Integrationsaufgaben.

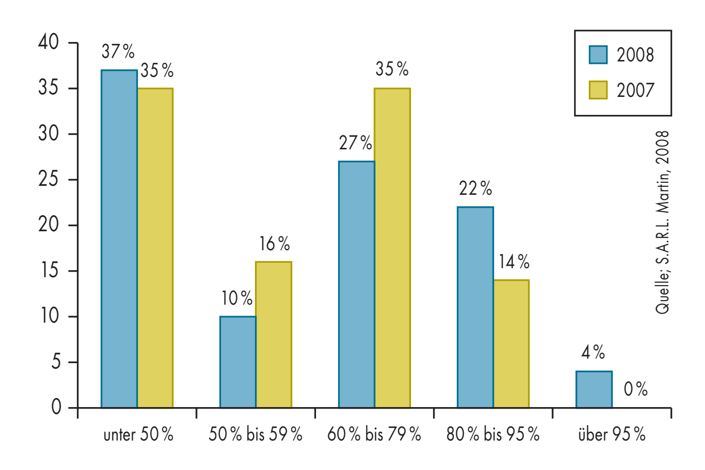
Peter Kempf von der Unicredit HVB Group stellte das Enterprise-Architekturmodell seines Hauses vor. Im Zentrum steht das TOGAF (The Open Group Architecture Framework), das sich aus den Ebenen Prozess-, Domain- (Service-Domänen) Integrations- sowie Systemmodell (technische Plattformen) zusammensetzt. Alle Modelle liegen in einem Repository. Mit diesem umfangreichen Ansatz will man die Services vereinheitlichen und vereinfachen.

Die Credit Suisse nutzt eine Java-Application-Plattform als Integrationsgrundlage für selbstentwickelte Anwendungen, die der zuständige Entwicklungschef Thomas Koch vorstellte. Zum Start vor rund neun Jahren war die Sache technisch geprägt. Das gilt noch heute, auch wenn handfeste wirtschaftliche Gründe (15 % niedrigere Betriebskosten pro Jahr) das bankeigene Konzept leiten. Zudem löst ein Kompositionskonzept das traditionelle Programmiermodell ab. Das Weblogic-Portal ermöglicht eine neue Klasse zusammengeführter Applikationen. Einerseits mindert diese Integrationstechnik die Komplexität der Hintergrundanwendungen, andererseits erzeugt sie neue Abhängigkeiten zwischen Programmen und wirft Versionierungsfragen und Ähnliches auf.

Dass Unternehmen ihre Integrationsarchitekturen nicht zwangsläufig aus lizenzpflichtigen Softwarekomponenten aufbauen müssen, zeigte ein Vortrag über die kommende EAI-Landschaft (Enterprise Application Integration) bei Union Investment. Ihre im Jahr 2002 eingeführte monolithische Middleware will die Kapitalanlagefirma durch eine Reihe von Open-Source-Komponenten ersetzen. Dazu gehören JBoss’ Application Server, die Messaging-Komponente JBossMQ, als J2EE-Umgebung der JCA Container, der Enterprise Service Bus Apache Servicemix sowie die Modellierungsumgebung jBPM. Eigenentwicklungen an der einen oder anderen Stelle sollen die Unternehmenstauglichkeit sicherstellen. Dies betrifft etwa den Einbau von Servicemix in JBoss. Die Erfahrungen sind überaus positiv. So erfüllen die Basiskomponenten problemlos die Anforderungen bezüglich Stabilität, und die Servicemix-Lösung brachte einen deutlichen Performancegewinn.

Andreas von Gunten, Chef der Schweizer Parx AG, bezweifelt, dass sich sich Unternehmen künftig überhaupt mit Integrationsfragen im eigenen Hause beschäftigen müssen. Er warb eindringlich für das SaaS-Konzept (Software as a Service). Die gehosteten Anwendungsdienste böten mindestens Integrationsfunktionen über Webservices API oder Mashups. Für komplexere Aufgaben stünden der Open-Source-Integrationsserver Jitterbit (www.jitterbit.com) sowie der On-demand-Service Boomi (www.boomi.com) bereit.

Parallel fand das Enterprise Architecture Management Forum statt. Unter dem Motto „Bauplan der IT: Optimale Unterstützung der Geschäftsprozesse durch die IT-Systemlandschaft“ erläuterten Vertreter namhafter Anwender (Deutsche Telekom, Münchener Rück, Kühne+Nagel, BMW), wie sie die IT-Architektur in ihren Unternehmen planen, überwachen und steuern. Die inhaltliche Nähe der beiden Veranstaltungen erschwerte leider das Zusammenstellen des eigenen Programms aus den parallel laufenden Vortragssträngen. (jd)



IIR Web-2.0-Kongress

Parallel zu den im Haupttext beschriebenen Foren lief in Wiesbaden der vierte IIR Web-2.0-Kongress. Das Programm umfasste Beiträge zur Anwendung entsprechender Techniken in der Unternehmenskommunikation und im kommerziellen Marketing. Neben den üblichen Referenten zu Social Networking (von Myspace, StudioVZ et cetera) erläuterten Vertreter von Sixt und Fraport den Einsatz von Wikis für die firmeninterne Zusammenarbeit. Beispielsweise ergänzt Skywiki des Frankfurter Flughafenbetreibers heute mit rund 1200 Artikeln das vorhandene Intranet. Es basiert auf dem ursprünglich für Wikipedia geschriebenen Mediawiki. Die wissenschaftliche Abrundung des Kongresses oblag Eero Hyvönen. Der Professor der Helsinki University of Technology stellte den Teilnehmern das National Semantic Web Ontology Project in Finnland (FinnONTO) sowie das Folgeprojekt Semantic Web 2.0 vor.

Natur als Vorbild für IT-Sicherheit

Jäger und Gejagte

Arno Puder

Mit der IT-Sicherheit ist es wie mit der Evolution: Nur wer flexibel bleibt, kann gewinnen. Das, so war auf der 17. RSA-Konferenz zu hören, gilt vor allem beim Kampf gegen Spam und Kreditkartenbetrug.

Mitte April fand die nordamerikanische Ausgabe der diesjährigen RSA-Konferenz in San Francisco statt. Mit 17 000 Teilnehmern konnte die wichtigste Konferenz zum Thema Sicherheit wieder einen neuen Rekord aufstellen.

Craig Mundie von Microsoft sieht das Social Engineering als die größte Herausforderung für die Sicherheit. Sicherheit ist oft orthogonal zur Privatsphäre einer Person und so fordert Mundie, was er „Situational Privacy“ nennt: In bestimmten Situationen werden lediglich zwingend notwendige Informationen freigegeben (z. B. Alterskontrolle), ohne jedoch die Identität des Benutzers preiszugeben.

Michael Chertoff von der Heimatschutzbehörde in den USA hob hervor, dass Cyberkriminalität insbesondere deswegen kritisch ist, weil eine einzelne Person großen Schaden anrichten kann. Er verwies auf die DDoS-Attacke gegen die estländische Regierung vom vergangenen Jahr.

Dauerbrenner Spam: Während es im Internet relativ einfach ist, Spuren zu verwischen, fällt es den Kriminellen wesentlich schwerer, Geldtransaktionen zu verschleiern. Kimberly Kiefer Peretti vom US-Justizministerium führte aus, wie die Kriminellen ein nach dem Paypal-Prinzip funktionierendes Bankwesen aufgebaut haben. Oft sind Gesetzeshüter machtlos, weil diese Organisationen über nationale Grenzen hinweg agieren. Paul Kocher, bekannt durch die Differential Power Analysis, zog in seinem Vortrag Parallelen zu evolutionären Prozessen, bei denen Jäger und Gejagte einander gegenüberstehen. Seiner Meinung nach kann im Kampf gegen Spam und Kreditkartenbetrug ein Vergleich mit der Natur neue Impulse bieten. So schützen sich in der Natur oftmals Gejagte, indem sie sich flexibel an neue Situationen anpassen.

Blu-ray evolutionärer Gewinner

Laut Kocher war das auch der Grund dafür, dass sich Blu-ray gegenüber HD-DVD durchgesetzt hat. Bei Blu-ray können neue Sicherheitsmechanismen quasi im Huckepack mit neuen Filmen auf einer Disk nachinstalliert werden, wohingegen HD-DVD keine Möglichkeit für dynamische Sicherheits-Updates bietet. Im Sinne eines evolutionären Prozesses erlaubt Blu-ray somit bessere Strategien gegen Piraterie.

Ein anderer Schwerpunkt der diesjährigen RSA-Konferenz war Virtualisierung. Sie entwickelt sich allmählich zum Heiligen Gral für das Management von IT-Infrastrukturen. Jedoch wirft insbesondere die mit ihr einhergehende Dynamik neue Sicherheitsfragen auf. Was passiert etwa mit Firewall-Policies, wenn das zugehörige System in ein anderes Subnetz migriert wird? Ebenso kann theoretisch das Gastsystem durch einen Fehler in der Virtualisierungssoftware den Host manipulieren. Andererseits kann die Virtualisierung bei der Umsetzung von Sicherheitskonzepten hilfreich sein. (ur)

„Privilege Escalation" unter allen Windows-Systemen

Im Sandkasten

Michael Dipper

Auch vor der trockenen Wüstenregion in den Vereinigten Arabischen Emiraten macht die Security-Szene keinen Halt. Datenbanken hacken, Cell-Prozessoren angreifen oder das Beschaffen von eigentlich verbotenen Privilegien funktioniert eben weltweit.

Die zweite Hack In The Box (HITB) in Dubai startete mit einer Keynote von Bruce Schneier, die den Zuhörer zum Nachdenken anregte: Sind von uns aufgestellte Modelle für Sicherheit, die wirklich erreichte Sicherheit und ein daraus entstehendes, subjektives Gefühl von Sicherheit immer gleich oder lassen wir uns nur von gefühlter Sicherheit beeinflussen? Basierend auf einer früheren Veröffentlichung (siehe *iX*-Link) stellte er dieses Thema unterhaltsam dar und zeigte Parallelen zwischen IT und Alltag.

Rodrigo Rubira Branco demonstrierte in seinem Vortrag „Hacking The Cell Architecture", wie sich die spezielle Architektur der Cell-Prozessoren für Angriffe ausnutzen lässt. Ursache hierfür ist der fehlende Speicherschutz im lokalen Speicher der einzelnen CPU-Kerne. Durch sichere Programmierung können derartige Angriffe zwar unterbunden werden, doch dies liegt allein in der Verantwortung des Entwicklers. Cell-Prozessoren finden sich in IBM-Blade-Servern.

Neue Wege, illegale Zugriffe auf Datenbanken zu erkennen, diskutierte der Oracle-Experte Alexander Kornbrust in „Practical Oracle Forensics". Im Fokus standen ungewöhnliche Quellen für Informationen wie das Listener Log, die Sequenznummern in (manipulierten) Audit Logs oder die Command History, die nur im Arbeitsspeicher liegt. Solche Informationen sind wichtig, wenn der Angreifer etwa der Datenbankadministrator ist und seine Zugriffe in Logdateien verschleiern kann.

In einem weniger technischen Vortrag zeigten Raoul Chiesa und Alessio Pennasilico das Auffinden und die Auswirkung möglicher Schwachstellen in sogenannten SCADA-Umgebungen. Hierunter versteht man die Messdatenerfassung und -verarbeitung in der Prozessautomatisierung. Wenn ein Angreifer Schwachstellen in den Regelkreisen der Elektrizitäts-, Gas- oder beispielsweise Wasserversorger ausnutzt, sind die Folgen meist fatal.

Übernahme von Identitäten

Ein Glanzlicht der Konferenz war der Vortrag „Token Kidnapping" von Cesar Cerrudo. Der Argentinier erläuterte, wie sich in allen aktuellen Windows-Versionen bis einschließlich Windows Server 2008 von einem eingeschränkten Benutzerkonto aus eine sogenannte „Privilege Escalation" durchführen lässt. Dies geschieht über Schwachstellen in Diensten, die das Recht zur Identitätsübernahme (impersonation) besitzen und unter Umständen im Besitz von Sicherheits-Token mit Rechten des System-Accounts sind. Als Workaround empfiehlt Cesar Cerrudo derzeit, Dienste wie den IIS unter einem lokalen Benutzerkonto und nicht als „lokalen Dienst" zu starten. Microsoft bestätigte mittlerweile die Schwachstelle und arbeitet an entsprechenden Patches (siehe *iX*-Link).

„Skyper" von „The Hacker's Choice" (thc.org) gab ein Update zum GSM-Projekt, das das Abhören und Entschlüsseln von Handy-Verbindungen mit einfachster Hardware (circa 500 €) ermöglicht. Ziel des Projektes ist es, durch Ausnutzung von Schwachstellen der A5/1-Verschlüsselung jedes Gespräch und auch SMS-Verbindungen binnen 30 Sekunden zu knacken. Die dazu erforderlichen Rainbow-Tables sind mehr als 2 TByte groß und derzeit zu rund 75 % berechnet. Sie sollen nach Fertigstellung zum Download angeboten werden. Überdies plant das Projekt ein Web-Interface, über das man Verbindungsmitschnitte hochladen und gleich online entschlüsseln kann.

Alle Vorträge der HITB Dubai finden sich auf der Konferenzseite (www.hitb.org). (ur)

iX-Link ix0806019

„De-Perimeterisierung“ auf dem Vormarsch?

Porös



Reinhard Wobst

Wenn Geschäftskommunikation auf immer stärkerer Vernetzung fußt, ist es schwierig, das Unternehmensnetz gegen Gefahren abzuschotten. Die Allzweckwaffe Verschlüsselung mag zwar gegen manchen Missbrauch helfen, hat aber andere Nachteile.

Der bedeutende Treff der Sicherheitsszene, die Infosecurity Europe 2008, fand Ende April in der Olympiahalle in London unter Beteiligung von über 300 Ausstellern statt, mit zahlreichen Vorträgen und 12 500 Besuchern. Wieder einmal wurde klar, mit welch komplexen Problemen die Datensicherheit heute zu kämpfen hat. Besonders eindrücklich zeigte dies Geraint Price (Royal Holloway University of London) in seinem Vortrag „De-Perimeterisation: Fact or Fiction?“: Die früheren Modelle zur Absicherung des Datenverkehrs greifen nicht mehr, weil beim heutigen Stand der Vernetzung und der Mobilität die „Festungen“ verschwinden.

Alte Trust-Modelle greifen nicht mehr

Nicht nur durch Outsourcing und Vernetzung, sondern auch durch immer neue Kommunikationsformen und den stark angestiegenen Austausch geschäftlicher Informationen sind Wissen und Prozesse kaum noch lokal zu halten. Es gibt ständig neue Herausforderungen und technische Entwicklungen wie mobile Endgeräte und Flash-Speicher. Obendrein gehören die Endpunkte der Kommunikation oft anderen, was klassische Trust-Modelle über den Haufen wirft. Verschlüsselung allein ist nicht die Lösung, denn das Keyhandling ist der schwache Punkt – vor allem, wenn es keine zentrale Autorität gibt. Eine konsistente Sicherheits-Policy wird so fraglich. Nach Price’ Ansicht steht die Sicherheitsforschung noch am Anfang.

Ähnliche Bedenken äußerte der bekannte Experte Bruce Schneier, der wieder einmal über den Gegensatz von Realität, gefühlter Sicherheit und Modell sprach. Die Einsicht, dass Rauchen schädlich ist (also die Anpassung des Modells und das Entwickeln einer gefühlten Bedrohung), habe Jahrzehnte gebraucht. Das Problem bei der Datensicherheit könnte sein, dass sich die Realität – das heißt die Technik – zu schnell verändert, als dass der Anwender sich anpassen könnte.

So gesehen war es logisch, dass eine Reihe von Ausstellern Produkte für ganzheitliche Sicherheit anboten, etwa Devicelock, das Verschlüsselung auf externen Datenträgern erzwingt und die Synchronisation mit mobilen Geräten kontrolliert. Technisch beruht das Produkt auf einer Modifizierung des Active-Directory-Services, greift also nur in reinen Microsoft-Welten und ist auch nicht gegen qualifizierte Angreifer gefeit. Insbesondere wird das Keyhandling Drittanbietern wie PGP überlassen, doch PGP ist nicht darauf aus, den Rechner vor seinem eigenen Anwender zu schützen. Ähnliches gilt für Credant Technologies’ Produkte, die in Microsoft-Umgebungen die Verschlüsselung externer Datenträger erzwingen. Beide Produkte werden in vielen Top-500-Unternehmen eingesetzt.

Interessant war auch der Vortrag von Tomas Olovsson (AppGate Network Security) über den praktischen Einsatz von Open-Source-Software, der ihre sicherheitstechnischen und wirtschaftlichen Vorteile eindrucksvoll erläuterte. (ur)

Was die RFID-Einführung in der Praxis behindert

Nutzen verteilen

Barbara Lange

Wenn mehrere Unternehmen in RFID-Projekten kooperieren, entstehen ganz neue Fragen: Welche Daten sollte man für andere freigeben? Wie aus den Riesen-Datenmengen handhabbare Informationen generieren? Im Projekt „Ko-RFID – Kollaboration und RFID“ arbeiten Industrie und Wissenschaft zusammen.

Herausfinden will man, warum die Einführung von RFID schleppender läuft, als es der Hype vor einigen Jahren hätte vermuten lassen. Ein Grund könnte sein, dass Kosten und Nutzen ganz unterschiedlich auf die einzelnen Partner verteilt sind. Wie man die gleichmäßig auf alle Beteiligten verteilen kann, soll das von BMWi mit fünf Millionen Euro geförderte Projekt „Ko-RFID – Kollaboration und RFID“ herausfinden.

Beteiligt sind die Humboldt-Universität und die Technische Universität aus Berlin, die Otto-von-Guericke-Universität Magdeburg, Gerry Weber International AG, Gustav Wellmann GmbH & Co. KG, Daimler AG und die SAP AG. Sie trafen sich Mitte April zur zweiten Jahreskonferenz in der Berliner Humboldt-Universität.

Hohe Investitionen am Anfang

Dass die Vorteile für die einzelnen Unternehmen sehr unterschiedlich sind, fanden die Wissenschaftler durch eine Umfrage in der Automobilbranche heraus. Für die Zulieferer zählt vor allem der Wettbewerbsdruck bei der Entscheidung für RFID. Auch gibt es in der Pilotphase hohe Kosten, und der Nutzen zeigt sich erst viel später, wie ein Vertreter von Gerry Weber in einem Praxisbericht erläuterte.

Mit einem Ko-RFID-Empfehlungs-Tool haben die Wissenschaftler ein Werkzeug entwickelt, das Unternehmen beim Ermitteln von Nutzen und Risiko von RFID-Projekten unterstützt.

Eine Herausforderung für die Forschung ergibt sich auch aus den großen Datenmengen, die RFID-Systeme erzeugen. Vom Datenmanagement berichtete Gregor Hackenbroich, Research Program Manager bei SAP Research. Ziel ist es, Suchanfragen wie „Wo ist eine bestimmte Warenlieferung gerade, und sind auch alle bestellten Produkte dabei?“ schnell zu beantworten, was gar nicht so leicht ist, vor allem, wenn die Fragen nicht zur Datenbankstruktur passen.

Als Architektur für das Datenmanagement sind technisch möglich: strukturierte P2P-Netzwerke oder die zentrale Datenhaltung in einem Knoten. Machbar ist ebenfalls, dass ein zentraler Knoten die Indizes für Objekte vorhält, eine Variante, die EPCglobal mit dem Object Name Server (ONS) favorisiert.

Vom Data-Mining berichteten Myra Spiliopoulou und Florian Kähne von der Otto-von-Guericke-Universität Magdeburg: Wie aus den verteilt liegenden Daten Informationen generieren? Unternehmen sollten keine Rohdaten aus RFID-Prozessen freigeben, sondern nur aggregierte Daten, da man selbst anonymisierte Daten wieder de-anonymisieren kann. Derzeit beschäftigt man sich damit, wie viel Datenverlust dabei akzeptabel ist. In einem nächsten Schritt wollen die Wissenschaftler untersuchen, ob sich aus den Daten Informationen generieren lassen, die die Unternehmen, die ja auch Konkurrenten sind, gar nicht offenlegen wollten. (ur)

Identitätsmanagement unterstützt Compliance

Rollenspiele

Susanne Franke

Dass Unternehmen auch beim Identitätsmanagement nicht an Themen wie Governance und Compliance vorbeikommen, zeigten die Beiträge der diesjährigen European Identity Conference 2008.

Zur European Identity Conference, die in diesem Jahr zum zweiten Mal stattfand, kamen insgesamt 450 Teilnehmer (20 Prozent mehr als im Vorjahr) aus 23 Ländern sowie 50 Aussteller nach München. Mit dabei waren die „Großen“ wie CA, IBM, Microsoft, Oracle, Novell oder Sun, aber auch kleine Unternehmen.

Mit Vorträgen von rund 130 Sprechern und Diskussionsrunden bot die Veranstaltung einen breiten Überblick sowohl über den Status Quo im Identity- und Access-Management (IAM) als auch über die praktische Umsetzung und die Trends.

Eines der vorherrschenden Themen war der Trend zu „Identity 2.0“. Mittlerweile sind die Standards OpenID 2.0, Infocards auf der Basis der Web-Service-Spezifikationen sowie SAML (Security Assertion Markup Language) vorhanden und laut Veranstalter Martin Kuppinger dabei, „Teil des wirklichen Lebens“ zu werden. Die Standards seien trotz noch offener Implementierungsfragen zunehmend interoperabel, so der Analyst in seiner Keynote, und Anbieter wie IBM, Microsoft, Novell, Yahoo, AOL und Google unterstützen alle bereits Identity 2.0 in ihren Produkten.

Der Identitäts-Guru Kim Cameron von Microsoft stellte in seiner Keynote ein Identity Metasystem Model vor, dessen Grundlage die Nutzung von Identity-Netzwerken ist. Das bedeutet, dass für die Authentifizierung unterschiedliche Attribute oder „Claims“ herangezogen werden, und zwar je nach Anwendung und Kontext. Dies können Name, Adresse, Kennwort sein, aber auch Rolle.

Er plädiert außerdem für ein Framework mit Protokollen, über die verschiedene Identity-Systeme interagieren und kontextspezifische Identity-Tokens für Online-Transaktionen austauschen können. Als zentrales Repository für die persönlichen Benutzerdaten müsse nicht etwa Microsoft oder ein anderer Anbieter infrage kommen, sondern eher eine Vielzahl an öffentlichen und privaten Institutionen, die die Identitäten verwalten.

Bewusstsein für Datenschutz gefordert

Marit Hansen, Leiterin des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, mahnte in einer Diskussion zur Zukunft der Web-Identität das Bewusstsein für Vertraulichkeitsprobleme mit digitalen Identitäten an und stellt die Frage, ob die sogenannten Trusted Authorities Behörden sein sollten, private Unternehmen oder vielleicht gar ein ISP. Konflikte kann es auch im internationalen Umfeld geben, denn die Datenschutzgesetze unterscheiden sich in den verschiedenen Ländern voneinander.

Als zweitwichtigsten Trend machte Kuppinger in seiner Keynote das Thema GRC (Governance, Risk Management, Compliance) aus. Die vorhandenen Werkzeuge für GRC dienen der Verwaltung von digitalen IDs, dem Business Role Management (etwa der Rollenvergabe an Nutzer), der Vergabe von Zugriffsrechten für Rollen, der Funktionstrennung (Segregation of Duties) oder dem Auditing-Bereich. Die Voraussetzung für den Erfolg von GRC jedoch ist die Unterstützung durch ein starkes Identity- und Access-Management, so Kuppinger. (ur)

ConhIT 2008: eGK-Testlauf abgebrochen

Hindernislauf

Barbara Lange

Spätestens mit der Einführung der elektronischen Gesundheitskarte müssen IT-Systeme und Menschen in Krankenhäusern, Arztpraxen, Apotheken sowie Krankenkassen zusammenarbeiten. Der Weg dorthin scheint weiter denn je.

Top-Thema der dreitägigen Kongressmesse ConhIT Anfang April in Berlin war die elektronische Gesundheitskarte (eGK). Gleich am ersten Tag kam der Hammer: Mitte März haben die Ärzte in Flensburg den Testlauf der elektronischen Gesundheitskarte abgebrochen, berichtete der Projektleiter der Testregion Schleswig Holstein, Jan Meincke. Der Grund: Die Eingabe der PIN ist zu kompliziert für ältere und chronisch kranke Patienten – 75 % von 7553 Testpatienten schafften das nicht und sperrten ihre Karte. Die PIN ist aber notwendig, da die Patienten die Eingabe von freiwilligen Notfalldaten der Karte autorisieren müssen.

Darüber hinaus gab es noch andere Projektprobleme, zum Beispiel falsche Zertifikate bei den ausgegebenen Heilberufeausweisen und daraus resultierende Verzögerungen.

Auch wenn sich die Gesundheitsbranche mit derlei Widrigkeiten herumschlagen muss, an der grundsätzlichen Notwendigkeit von Gesundheitskarte samt Telematikinfrastruktur zur Gewährleistung eines rechtskonformen und abrechnungssicheren Verfahrens zweifelte niemand der 150 Aussteller und rund 2500 IT-Verantwortlichen, die nach Berlin gekommen waren. Veranstalter der ConhIT waren der Verband der Hersteller von IT-Lösungen für das Gesundheitswesen e. V. (VHITG) und die Messe Berlin.

Umstritten ist allerdings, ob das Rollout, wie von der Bundesregierung geplant, unbedingt noch in diesem Jahr stattfinden muss – aufgrund technischer Probleme, aber auch mangels Akzeptanz etwa bei Ärzten und Patienten.

Dass sektorenübergreifende IT-Systeme die vielfach noch vorhandenen isolierten medizinischen Systeme ablösen werden, ist ein notwendiger Trend, mit allen dazugehörenden Problemen: Interoperabilität, Standardisierung oder Archivierung. Die Produkte und Aussagen der Aussteller, darunter Siemens Medical Solutions, Agfa Healthcare, iSOFT, SAP, HP, Microsoft und Sun Microsystems, spiegelten das wider.

Ohne Interoperabilität geht nichts

Als Beispiele für die Interoperabilität zeigten Partner des Projekts EPA.nrw den Weg einer elektronischen Patientenakte vom IT-System des Arztes über das Krankenhaus bis zum Patienten. Die Deutsche Rentenversicherung präsentierte einen Implementierungsleitfaden für den eReha-Entlassungsbericht zum Austausch ärztlicher Berichte. Als Europa-Premiere stellte Microsoft ein Krankenhaus-Informationssystem namens Amalga vor, das die freie Kombination aller bislang isolierten IT-Lösungen in den Bereichen Klinik, Finanzen und Verwaltung ermöglichen soll.

Zwischenzeitlich zeigt sich noch eine ganz andere Entwicklung, die die Planer der eGK 1994 noch gar nicht absehen konnten: Warum nicht die Gesundheitsdaten online stellen? In den USA kündigen sich hier neue kommerzielle Angebote an, zum Beispiel von Google und Microsoft. Auch der „Homo Handykus“ könnte mithilfe der Near Field Communication von Handys mobile Vorlieben entwickeln. (ur)

MySQL Conference & Expo 2008

Mehr fürs Geld

Markus Franz

Im Vordergrund der diesjährigen MySQL Conference standen die Übernahme der freien Datenbank durch Sun und die weitere Entwicklung des Produkts.

Im kalifornischen Santa Clara fand Mitte April die Hauskonferenz des RDBMS-Anbieters MySQL statt, auf der sich 2000 Besucher und über 50 Aussteller drängelten. Die wichtigste Frage in diesem Jahr: Wie geht es mit MySQL nach der Übernahme durch Sun Microsystems weiter? Marten Mickos, Ex-CEO und nun Senior Vice President der Database Group bei Sun, gab darauf im MySQL Partner Meeting eine Antwort: Die Übernahme wird keine großen, ungeplanten Änderungen an Produkten oder der Zusammenarbeit mit der Community bringen. MySQL werde in Zukunft aber verstärkt einzelne Features ausschließlich in der kommerziellen Version enthalten – zum Beispiel Teile der für MySQL 6.0 geplanten Backup-Funktion.

Schwartz lobt Open Source

Als weitere wichtige Ankündigung wurde MySQL 5.1 präsentiert, das kurz vor der Veröffentlichung steht. Der aktuelle Release Candidate und die endgültige Version sollen erheblich stabiler und schneller sein als Version 5.0, mit der laut Mickos das MySQL-Team selbst nicht zufrieden war. Während der Konferenz erschien MySQL Workbench als neues Produkt, von dem es eine Community- und eine Enterprise-Variante gibt. Hierbei handelt es sich um einen Designer, mit dem man grafisch die MySQL-Datenbank entwickeln, verwalten und komplexe Tabellen modellieren kann.

In seiner Keynote sang Suns CEO Jonathan Schwartz ein Loblied auf die Open-Source-Szene: Er sei seit seinem Antritt bei Sun vor zwei Jahren ein starker Kämpfer für offene Standards. Mit MySQL habe eine großartige Zusammenarbeit begonnen, die für die beiden Unternehmen und ihre Kunden exzellente neue Möglichkeiten biete. Einerseits profitierten die Open-Source-Anhänger durch Suns Investitionen und jahrelange Erfahrung; andererseits gebe es mit MySQL für Unternehmen nun einen integrierten Open-Source-Stack.

Weitere Veröffentlichungen während der Konferenz kamen von Zmanda, die eine neue Version der Backup-Lösung für MySQL ankündigten, und von Kickfire. Dieser Sponsor der Konferenz verkündete die Partnerschaft mit MySQL und weiteren Datenbankanbietern. Er kündigte eine integrierte Business-Intelligence-Lösung an, die als Appliance mit MySQL ausgeliefert werde.

Im Vortragsprogramm erklärte Sebastian Bergmann das Testen von Datenbankanwendungen mit PHPUnit und DBUnit. Joshua Drake zeigte, was MySQL von PostgreSQL lernen kann. Robin Schumacher und Rob Young stellten in „The Future of MySQL“ die Entwicklung der Datenbank in den nächsten fünf Jahren vor: einerseits hin zur universellen Basis für Open-Source-Projekte, andererseits in den High-End-Bereich für skalierbare Unternehmensanwendungen. Dabei gab er einen Ausblick auf den kommenden Load Balancer und den Query Analyzer.

Innobase, das nun zu Oracle gehört, stellte die neue Version seiner Storage Engine für MySQL vor. Damit können Anwender über den Pluggable-Storage-Mechanismus von MySQL 5.1 das transaktionsfähige InnoDB-Backend einsetzen. (ck)

iX-Veranstaltungen

www.ix-konferenz.de.

Auch in diesem Jahr konnten wir unsere langjährigen Autoren Christoph Leisegang und Stefan Mintert für ein Seminar zum Thema **Web 2.0 mit Ajax** gewinnen. Im Juli und August finden in Stuttgart, München und Frankfurt/M. zweitägige Workshops statt. Die Teilnehmer beherrschen danach die technischen Grundlagen zur selbstständigen Entwicklung von Webanwendungen mit Ajax. Aufpassen: Bis zum 15. Juni greift noch der Frühbucherrabatt von 20 Prozent.

Mit denselben Referenten findet am 22./23. Juli in München ein Seminar zum Thema **XML-Verarbeitung mit XSLT** statt (www.ix-konferenz.de).

Ausgeweitet haben wir auch die Zusammenarbeit mit Holger Schwichtenberg, und zwar in Sachen Seminare zur **.Net-Softwareentwicklung**, die mittlerweile die ganze Spannbreite der Programmierung mit Microsofts Framework abdecken.

Wirklich beeilen muss sich, wer noch in den Genuss des Frühbucherrabatts für die **Forensik-Workshops** kommen will – der gilt nämlich nur noch bis zum 15. Mai. Ähnlich schnell sollten alle sein, die gerne einen Vortrag auf der **MedConf 2008** zum Thema Software- und Systementwurf für Medical Devices halten möchten. Die Einreichungsfrist endet am 16. Mai.

Neues Event-Format

Außerdem bietet *iX* ab sofort ein neues Veranstaltungsformat an: die ***iX*-Roadshows**. Sie ergänzen die *iX*-Konferenzen und -Workshops und verstehen sich als Präsentationsmöglichkeit für unsere Medienpartner. Die ersten Roadshows sind den Themen Anforderungsmanagement, Testen, Projektmanagement und UML-Modellierung gewidmet. Die Teilnahme ist kostenlos; die Roadshows werden in mehreren Städten in Deutschland stattfinden.

Prozessautomatisierung für das RZ

CA erweitert mithilfe von Opalis sein Angebot für die Rechenzentrumsautomatisierung. Die Software von Opalis hat man bereits in einige Produkte wie Spectrum und E-Health integriert. Durch das jüngste Vertriebsabkommen erweitert das Unternehmen nun die Suite von IT-Prozessautomationslösungen. Die Software des Vertriebspartners eignet sich insbesondere für die Automation der Prozesse und Workflows kritischer IT-Aufgaben wie Virtualisierung, Provisionierung, ITIL-konforme Prozesse (ITIL, IT Infrastructure Library), Disaster Recovery, Konsolidierung und Security. Neben CA arbeitet das kanadische Unternehmen auch mit EMC, Microsoft, IBM, VMware, Bladelogic, BMC und HP zusammen.

Vollständiges Inventarmanagement

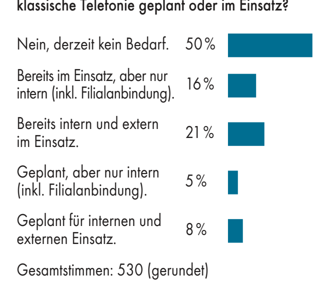
Mit Version 7.2.4 aktualisiert Touchpaper seine IT Business Management Suite (ITBM). Ein Asset-Management-Prozesspaket soll den gesamten Prozess rund um die IT-Inventarisierung verwalten – vom Beschaffen bis zum Entsorgen. Anschaffungen lässt sich die IT-Abteilung vom Budgetverantwortlichen genehmigen. Das Touchpaper-System generiert den Auftrag zum Einkauf und leitet ihn an die Finanzabteilung weiter. Die Software überwacht anschließend die Lieferung und, falls erforderlich, die Installation und Konfiguration der neuen Geräte. Neues IT-Inventar erscheint als Configuration Item (CI) in der Configuration Management Database (CMDB). Im Falle der Ausmusterung liefert das Prozesspaket den Nachweis, dass der Entsorgungsprozess entsprechend den EU-Richtlinien erfolgt, etwa gemäß WEEE (Waste Electrical and Electronic Equipment). Als Vorbild für das ITBM diente ITIL v3.

Agentenfreies Server-Monitoring

Mit Experttracer for Server mischt das Darmstädter Softwarehaus Servicetrace im Tool-Markt zur Überwachung der Server-Ressourcen mit. Die Software analysiert agentenlos Windows-, Unix- und Linux-Systeme in Bezug auf CPU- und Speicher-Auslastung, Verfügbarkeit, Netzwerkkartenbelastung und Zahl der angemeldeten Benutzer. Das Server-Monitoring zur Darstellung entscheidungsrelevanter Informationen erfolgt zentral per SNMP. Mittels einer Scan-Funktion lassen sich laut Herstellerangaben zusätzliche Server-Systeme minutenschnell in die Überwachung einbinden. Die Darmstädter Firma bietet neben der Server-Monitoring-Lösung im Rahmen des Servicetracer-Angebots auch Module zur Netzwerküberwachung, einen End-to-End-Roboter für das Applikations-Monitoring auf der Client-Ebene und eine zentrale Managementeinheit an. Die Plattform umfasst eine SAP-Komponente.

iX-Umfrage: 50:50 für VoIP

Auf Voice over IP gut verzichten zu können meint rund die Hälfte (49 %) der Teilnehmer unserer Online-Umfrage, die parallel zu Ausgabe 5/08 auf www.ix.de lief. Dafür ist Internet-Telefonie für die externe oder interne Kommunikation bereits bei 38 % der Antwortenden im Einsatz, 13 % haben VoIP auf der To-do-Liste – insgesamt also ein klares Patt. Details sind der nebenstehenden Grafik zu entnehmen. Am 14. Mai startet die neue *iX*-Umfrage, es geht um eigene Erfahrungen mit Viren und anderer Malware.



KURZ NOTIERT

Beworben: Das Potsdamer Hasso-Plattner-Institut (HPI) ließ an allen Gymnasien der alten Bundesländer zusammen mit der Jugendzeitschrift „SPIESSER“ Postkarten auslegen, die auf den HPI-Studiengang „IT Systems Engineering“ hinweisen. Abiturienten des aktuellen Jahrgangs können sich bis zum 15. Juli um einen der 80 Studienplätze bewerben (www.hpi.uni-potsdam.de/bachelor).

SVG-Viewer: Examotion hat die Version 1.0 seines SVG-Viewers Renesis gegenüber dem Vorgänger 0.7 völlig neu geschrieben. Er unterstützt CSS 2.1, DOM 3 Core und Events sowie SVG 1.1. Erhältlich ist das frei verfügbare Tool bei www.examotion.com sowohl als Stand-alone-Version für XP und Vista wie als Internet-Explorer-Plug-in.

Altes Internet: Anders als zahlreiche Medien berichteten, ist das Internet nicht erst 15 Jahre alt. Das vielfach gemeldete Jubiläum des WWW als Teil des Internet leitet sich davon ab, dass Tim Berners-Lee und Robert Cailliau von ihren Chefs am Genfer Kernforschungszentrum CERN am 30. April 1993 die Erlaubnis erhielten, ihre Webbibliothek *libwww* als freie Software weiterzugeben.

Wikipedia-Buch: Im September will das Bertelsmann Lexikon Institut, das zum Wissen Media Verlag gehört, für 19,95 € ein einbändiges Wikipedia-Lexikon herausgeben. 50 000 in den vergangenen anderthalb Jahren häufig nachgefragte Begriffe soll es enthalten.

Kartenformat: Google hat im April die XML-Anwendung KML an das Open Geospatial Consortium (OGC) übergeben, wo die Geodatensprache jetzt als offener Standard betrieben wird (www.opengeospatial.org/standards/kml).

SGI baut seinen RAID-Speicher aus

InfiniteStorage 4600 heißt SGIs neue Generation von RAID-Speichern, die speziell für datenintensive Anwendungen mit hohen I/O-Anforderungen und die Konsolidierung komplexer Datenbestände ausgelegt sind. Sie bietet 16 redundante Anschlüsse mit einer Übertragungsgeschwindigkeit von 4 GBit/s für Fibre-Channel-Laufwerke. Damit ist sie doppelt so schnell wie der Vorgänger, die InfiniteStorage 4500. Die 4600 kommt auf bis zu 6000 MByte/s, wenn der Host sequenziell 512 KByte große Datenpakete liest – was in der Praxis selten vorkommt. SGI gibt bei 4 KByte großen Anfragen an ein Fibre-Channel-Laufwerk eine kontinuierliche Leistung von 175 000 Input/Output-Operationen je Sekunde an.



Plattenweise: Bis zu 256 Terabyte Massenspeicher kann das InfiniteStorage 4600 von SGI aufnehmen (Abb. 1).

Das RAID-System hat in seiner Basisversion Kapazität für 256 Fibre-Channel- oder SATA-Laufwerke. Insgesamt sind Speichervolumina bis zu 256 Terabyte denkbar. Die InfiniteStorage 4600 beherrscht die RAID-Level 1, 3, 5, 6 und 10 und bietet redundante I/O-Pfade nebst automatisierten Failover-Prozessen. Erste InfiniteStorage 4600 Arrays sollen beim Norddeutschen Verbund für Hoch- und Höchstleistungsrechnen (HLRN) in Betrieb gehen. Der HLRN betreibt seine Supercomputer an zwei Standorten: dem Konrad-Zuse-Zentrum für Informationstechnik in Berlin (ZIB) und dem Regionalen Rechenzentrum für Niedersachsen in Hannover (RRZN), wo das RAID-System zum Einsatz kommen soll. Die Anschaffung eines InfiniteStorage 4600 schlägt mindestens mit 105 000 Euro zu Buche (www.sgi.com/products/storage/).

Nikolai Zotow

iX-Link ix0806028

Neues Rack-Format für Rechenzentren

Mit einem neuen Rack-Format will IBM die Kosten für Stromversorgung und Kühlung im RZ reduzieren. Das Angebot richtet sich vornehmlich an Betreiber von Web-2.0-Diensten oder großen Clustern.

Die iDataPlex getauften Racks sind nur etwa 70 cm tief (27,6 Zoll) – normale 19-Zoll-Racks bringen es fast auf 1,20 m – und sind deshalb leichter zu kühlen. Laut IBM passen doppelt so viele Systeme als sonst ins Rack, bei 5-facher Rechenleistung sinkt die Energieaufnahme um 40 %. Mit einer flüssigkeitsgekühlten Rücktür (Rear Heat Exchanger) soll man sogar mit Zimmertemperatur auskommen.

Bislang bietet IBM das iDataPlex-System für Intel-Server an. Ein 2 U hohes Rechnermodul enthält zwei Dual-Xeon-Systeme mit gemeinsamer Stromversorgung und Lüftung. Zusätzliche Speicherknoten bringen auf 3 U maximal zwölf 3,5-Zoll-Festplatten mit je 750 GByte unter.



Schlankheitskur: Die nur 70 cm tiefen Schränke lassen sich effektiver kühlen als die sonst 120 cm tiefen 19-Zoll-Racks (Abb. 2).

In Deutschland soll iDataPlex zum Jahresende verfügbar sein. Die Preise lägen zwischen 150 000 und 300 000 US-$, damit 20 bis 25 % unter einer vergleichbaren Lösung mit 1-U-Servern, betont der Hersteller. *Nikolai Zotow*

Standard-Schnittstelle für Flash-Speicher

Die vor einem Jahr von Dell, Intel und Microsoft ins Leben gerufene Non-Volatile Memory Host Controller Interface (NVMHCI) Working Group hat die Version 1.0 der NVMHCI-Spezifikation vorgelegt. Sie definiert eine einheitliche Programmierschnittstelle für Flash-Speicher. Geht es nach dem Willen der Initiatoren, soll NVMHCI in jeden PC Einzug halten, ähnlich wie zuvor das Enhanced HCI für USB 2.0 oder das Advanced HCI für SATA-Festplatten. Entwickler müssen allerdings von Intel eine Lizenz erwerben.

iX-Link ix0806028

Festplatten-Neuheiten bei Hitachi, Western Digital und Fujitsu

Eine Server-Festplatte mit 450 GByte Kapazität bringt Hitachi auf den Markt. Die Ultrastar 15K450 (siehe *iX-Link*) lässt ihre vier Scheiben mit 15 000 U/min rotieren und erreicht dadurch einen Datendurchsatz von 100 bis 160 MByte/s (innen/außen) bei einer durchschnittlichen Latenz von nur 2 ms. Allerdings bezahlt der Nutzer die hohe Leistung mit entsprechendem Energiebedarf: Die SAS-Version des Laufwerks schluckt im Betrieb 17,2 und im Leerlauf 13,3 Watt, die 4-GBit-Fibre-Channel-Variante sogar noch etwas mehr. Der Hersteller will die Laufwerke noch im zweiten Quartal ausliefern; Preise nannte er bislang noch nicht (www.hitachigst.com).

Kühlkörper integriert

Western Digital verpackt in der „VelociRaptor“ eine 2,5" große SATA-Platte mit 10 000 U/min und 300 GByte in ein Gehäuse mit 3,5-Zoll-Formfaktor – den Rest des Raums nimmt ein „Icepack“ getaufter Montagerahmen mit Kühlkörper ein. Das laut WD „schnellste SATA-Laufwerk der Welt“ überträgt bis zu 120 MByte/s. Angesichts dessen ist sein Stromverbrauch durchaus moderat: 6,1 Watt im Betrieb, 4,5 im Leerlauf und 0,4 im Schlafmodus. Die Zuverlässigkeit beziffert der Hersteller mit einer MTBF von 1,2 Millionen Stunden (www.wdc.com/de/).

Seine Notebook-Festplattenserie MHZ2 CJ stattet Fujitsu mit einem Verschlüsselungs-Chip aus. Alle Daten auf der 320 GByte großen SATA-Platte lassen sich mit dem AES-Algorithmus (Advanced Encryption Standard) verschlüsseln. Anders als bei Software-Verschlüsselung – etwa mit TrueCrypt – bleibt der verwendete 256-Bit-Schlüssel jedoch sicher im Laufwerk. Zusätzlich beherrschen die Geräte sogenanntes schnelles Secure Erase: Alle Daten auf der Platte lassen sich innerhalb einer Sekunde löschen. Trotz der zusätzlichen Hardware und einer Rotationsgeschwindigkeit von 7200 U/min genehmigt sich die Platte beim Lesen und Schreiben nur 2,3 Watt. Zum Datendurchsatz macht Fujitsu bisher leider keine Angaben. Bis zum Jahresende will der Hersteller 2 Millionen Stück verkaufen; Lieferbeginn ist im Mai. Preise blieben ungenannt (www.fujitsu.com/us/services/computing/storage/hdd/mobile/mhz2320cj-sata.html).

iX-Link ix0806028

IBM verbessert Cluster-Fähigkeiten in Informix Dynamic Server 11.5

Ende April erschien Version 11.5 (Cheetah 2) des Informix Dynamic Server (IDS). Ein Schwerpunkt der Entwicklung seit Cheetah 1 war die vollständige Unterstützung von DML-Operationen (Data Manipulation Language) auf allen Knoten eines Clusters. Früher war das Schreiben (*INSERT, DELETE, UPDATE*) nur auf dem Master-Server erlaubt, auf alle anderen Cluster-Maschinen konnten Anwendungen ausschließlich lesend zugreifen. Hinter den Kulissen ist das weiterhin so, denn die Secondary Server leiten ab IDS 11.5 alle Schreibbefehle an den Chef des Clusters weiter, der sie ausführt und im Verbund weiterreicht. Entwickler müssen so nicht mehr zwischen Primary und Secondary Servern unterscheiden. Damit will IBM den Abstand zu Oracle und dessen Rapid Application Cluster verringern. Der Connection Manager *oncmsm* verteilt alle Client-Anfragen im Cluster auf die jeweils am wenigsten belasteten Rechner, während der ebenfalls neue „Connection Manager Arbitrator“ bei Ausfall des Primärknotens im Cluster automatisch einen Rechner auswählt, der die Aufgaben der defekten Maschine übernimmt.

Weitere Verbesserungen betreffen das Open-Admin-Tool. Diese im Browser laufende Anwendung erlaubt das Überwachen und Verwalten von Cluster-Rechnern (Hinzufügen, Entfernen). In Stored Procedures lassen sich dynamische Statements definieren und verwenden, *BIGINT* und *BIGSERIAL* kommen als neue Datentypen hinzu. Mit IDS 11.5 bietet IBM erstmals eine Informix-Version für Mac OS X an. Die Firma sieht mögliche Einsatzbereiche vor allem bei (Online-)Spielen und in der Grafik- sowie Prepress-Branche. Für Mac OS X 10.5 (Leopard) stellt sie wie für Linux und Windows eine „Developer Edition“ des IDS zum Herunterladen zur Verfügung (s. *iX*-Links). Sie ist nicht funktional eingeschränkt, darf jedoch nur für Entwicklungsarbeiten, nicht in der Produktion genutzt werden.

MySQL-Funktionen weiterhin in allen Produktvarianten vorhanden

Kurz nachdem Marten Mickos auf der MySQL-Conference (s. Bericht auf S. 23) angekündigt hatte, in Zukunft seien manche Neuerungen der freien Datenbank nur noch in der kommerziellen Version verfügbar, korrigierte Suns Chef Jonathan Schwartz: Weiterhin würden alle MySQL-Funktionen in der freien („Community Edition“) und in der kommerziellen Variante zur Verfügung stehen.

Inzwischen gibt es einige Informationen, was die Entwickler für kommende MySQL-Versionen planen (s. *iX*-Link). 6.0 soll Ende des Jahres fertig werden und die neu geschriebene transaktionsfähige Falcon-Engine sowie eine Backup-Funktion mitbringen, die für alle Backends funktioniert. Verbesserungen im Optimierer sollen Subqueries beschleunigen.

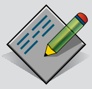
Für folgende 6er-Versionen ab 2009 planen die Entwickler Fremdschlüssel-Support für sämtliche Speicher-Engines, *SIGNAL* in Stored Procedures und schnellere Cursor. Erst ab MySQL 7.x wird es die von anderen Produkten bekannten *ROLEs* geben, die die Benutzerverwaltung erleichtern. Ebenfalls für diese Versionen ist Datenverschlüsselung für Tabellen und Spalten geplant.

iX-Link ix0806029

SAP engagiert sich für Virtualisierung

Mitte April verkündete SAP die Gründung einer Community zur IT-Virtualisierung. Deren Ziel: Das Entwickeln von Virtualisierungstechniken, die sich an den Geschäftsprozessen orientierten. Dabei will man alle Ebenen der Virtualisierung abdecken – vom Netzwerk über CPU, Server, Speichersystem bis hin zum Desktop. Zu den Gründungsmitgliedern zählen AMD, Cisco, Citrix, EMC, HP, Intel, Network Appliance, Novell, Red Hat, Sun und VMware. Schon heute stehen den SAP-Anwendern unterschiedliche Virtualisierungsansätze zur Verfügung. Beispielsweise können sie Applikationen auf Basis von VMwares ESX-Server in Produktivumgebungen mit 64-Bit-Windows und Linux nutzen. Gemeinsam mit ihrem bevorzugten Linux-Lieferanten Novell arbeiten die Walldorfer daran, dessen Virtualisierungstechniken für SAP-Programme unter Suse Linux Enterprise anbieten zu können. Aus dem eigenen Hause stammt der auf Netweavers J2EE-Engine basierende ACC (Adaptive Computing Controller). Mit der Managementkomponente lassen sich die Laufzeitdaten logischer und physischer Landschaften überwachen, Anwendungsmodule starten, stoppen und verlagern sowie Hardwareressourcen bestimmten Komponenten zuordnen. Nach offizieller Lesart ergänzt der ACC andere auf Hypervisor-Technik aufbauende Virtualisierungslösungen à la VMware, beispielsweise im Rahmen von Wartungsarbeiten am Betriebssystem.

KURZ NOTIERT



Funkfunktion: Output-Managementspezialist Streamserve hat seine Software mit einem RFID-Modul ausgestattet. Es erlaubt Unternehmen, RFID-Tags zu kodieren und über spezielle Drucker auszugeben. Die Komponente unterstützt verschiedene Tag-Typen, Kommunikationsprotokolle, elektronische Produktcodes und Drucker.

Größere Auswahl: Mit der webbasierenden Projektmanagementsoftware Projektron des gleichnamigen Herstellers lassen sich jetzt auch Angebote erstellen. Den einzelnen Positionen kann der Benutzer Rabatte und Zusatzinformationen sowie erläuternde Textblöcke zuweisen (etwa zu Klauseln). Eine Liste über alle laufenden Angebote gibt Auskunft über zu erwartende Einnahmen und Bindungsfristen.

Prüfsiegel: SAP hat die Archivschnittstelle des ECM-Anbieters d.velop für den Netweaver 7.0 zertifiziert. Über d.link for archivelink 2.4 lassen sich große Datenmengen im ECM-System d.3 revisionssicher ablegen. Die Zertifizierung bezieht sich auf die Funktionen HTTP Content Server, OLE Front-end, Barcode BAPI und Solution Manager Ready.

Für Entwickler: EMC offeriert neue OEM-Software für Content-Management, Dokumentenerfassung und XML-Datenmanagement. Jüngstes Mitglied der Documentum Content Server OEM Edition ist der XML-Store-Baustein. Er verwaltet XML-Daten wie technische Informationen und ermöglicht ihre gemeinsame Nutzung. Mit dem neuen Information Rights Management Software Development Kit lassen sich Sicherheitsfunktionen in Web-2.0-Anwendungen, SaaS-Umgebungen (Software as a Service) oder Arbeitsgeräte einbinden.

Lukratives CRM: Einer Gartner-Untersuchung zufolge soll der Umsatz mit CRM-Software im laufenden Jahr weltweit um 14,2 % auf ein Volumen von 8,9 Mrd. Dollar zulegen. Die Einnahmen in Nordamerika – mit 4,3 Mrd. Dollar der lukrativste Markt für die einschlägigen Anbieter – sollen bis 2012 auf 7,6 Mrd. Dollar steigen. Für Europa (2007: 2,6 Mrd. Dollar) prognostizieren die Analysten 2008 ein Marktvolumen von 3,9 Mrd. Dollar.

Wiki im Anflug: SAP möchte seine Portaltechnik mit einem Wiki veredeln. Als Basis dient Clearspace von Jive Software. Das Programm läuft auf dem hauseigenen J2EE-Server und wird als iView in der Portaloberfläche integriert. Ab Herbst soll eine Beta-Version verfügbar sein. Auf die Marktreife müssen die Anwender wohl noch rund ein Jahr warten.

Mobiles Geschäft: SAP und Research In Motion planen neuartige mobile Geschäftslösungen. Im Rahmen ihrer Zusammenarbeit wollen beide Unternehmen den mobilen Zugriff auf SAP-Geschäftsanwendungen über die Blackberry-Plattform ermöglichen.

Salesforce integriert Google Apps

Salesforce.com vermarktet Googles Office-Suite Apps als Teil der Anwendungsoberfläche seiner eigenen Mietsoftware. Dadurch sind die Nutzer beispielsweise in der Lage, eine E-Mail im Google-Postfach via Knopfdruck einem Datensatz im Salesforce-System zuzuweisen. Mit den Office-Werkzeugen lassen sich Angebote, Berichte und Ähnliches verfassen. Bislang stand den Salesforce-Anwendern lediglich ein Modul zur Verfügung, mit dem sich eine lokal installierte Office-Suite mit der On-Demand-Applikation koppeln ließ.

Mach mit neuen Fähigkeiten

Flexiblere Planungsprozesse sowie besser angebundene Fachverfahren über eine serviceorientierte Architektur (SOA) soll die neue Version von Mach Software bieten. Beispielsweise lassen sich mit dem für den Einsatz in öffentliche Verwaltungen und Non-Profit-Organisationen konzipierten Programm Finanzpläne in verschiedenen Versionen erstellen oder aufeinander aufbauen. An den aktuellen Wirtschaftsplan ist jeweils eine mittelfristige Finanzplanung gekoppelt. Zudem bekam Mach neue Dokumentenmanagementfunktionen.

Open Text überwacht den Dokumentenfluss

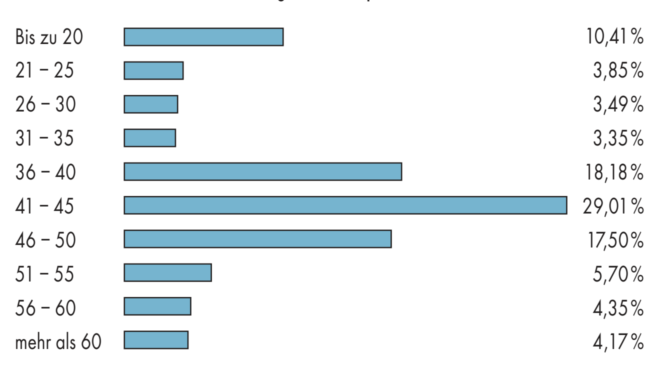
Auf der europäischen Kundenkonferenz Livelinkup Europe 2008 stellte das kanadische Softwarehaus Open Text seine Technik für das Transactional Content Processing (TCP) vor. Der sperrige Begriff umschreibt dokumentenbasierte Abläufe, wie sie beim Verarbeiten von Reklamationen, Anträgen oder Rechnungen entstehen. Die TCP-Software stellt die notwendigen Funktionen für Überwachung und Management hochvolumiger, weitgehend automatisierter und strukturierter Geschäftsprozesse zur Verfügung. Alle Inhalte verwaltet der Anwender mithilfe der Enterprise Library Services (zentrales Repository) über den gesamten Lebenszyklus. Zudem bindet das Produkt über Middleware Drittsysteme wie SAP in die Verarbeitung ein.

Docuware: Buntes Archiv

Seine Dokumentenmanagementsoftware hat Docuware mit einem farbenfreudigen Tiffmaker-Modul ausgestattet. Formulare lassen sich in der aktuellen Release 5.1 beim Druck gleichzeitig in Farbe archivieren. Weiterhin kann der Benutzer die Dokumente automatisch mit Rück- und zusätzlichen Seiten versehen. Für die Ablage selbst erstellter Belege übernimmt Docuware den Druckdatenstrom von Windows und teilt ihn in Einzeldokumente. Das System liest die Kategorisierungs- und Indizierungsinformationen aus und stellt sie in das Archiv. Optional hinterlegt das DMS auch Formulare oder Briefbögen.

Webworker arbeiten lange oder in Teilzeit

2800 zwischen 1970 und 1987 geborene Teilnehmer beteiligten sich an einer nicht repräsentativen Umfrage zu Arbeitsbedingungen, Gehältern und dem beruflichem Werdegang von „Webworkern“, die die Entwicklergruppe Webkraut (www.webkrauts.de) im Januar/Februar dieses Jahres durchgeführt hatte. Wie nebenstehender Zeichnung zu entnehmen ist, arbeiten die im und fürs Web Tätigen überwiegend zwischen 36 und 50 Stunden pro Woche. Als Kernkompetenz bezeichnen gut 72 % Markup-Sprachen wie (X)HTML und XML. Fast ebenso viele nennen Styling. Es folgen Backend-Programmierung mit knapp 61 % sowie barrierefreies Webdesign mit knapp 50 %. Flash-Entwickler haben an der Umfrage so gut wie nicht teilgenommen – vielleicht gibt es in Deutschland keine.



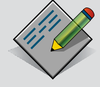
Circa 76 % der Teilnehmer arbeiten seit drei bis zehn Jahren in ihrem Beruf, gut ein Viertel selbstständig. Über 80 % der Webschaffenden ist mit ihrer Tätigkeit mindestens zufrieden. Ein Fünftel verdient im Jahr weniger als 10 000 €, was daran liegen kann, dass nicht alle Teilnehmer vollzeitbeschäftigt sind. Der Durchschnitt liegt nach den Antworten zwischen 30 000 und 35 000 € – wobei gilt, dass mit höherem Studienabschluss das Gehalt höher ausfällt. Frauen stellen lediglich ein Zehntel der Webworker; anders als im Vorbild der Befragung: Das Online-Magazin A List Apart hatte 2007 eine Befragung durchgeführt, die über 16 % weibliche Teilnehmer hatte. Die gesamte Auswertung steht auf der Ergebnisseite zum Download zur Verfügung (jendryschik.de/wsdev/umfrage/ergebnisse/).

Corinna wandelt Informationen in Wissen um

Die Karlsruher Firma living-e bringt mit Corinna (Corporate Intelligence Application) eine Plattform für die unternehmensweite Bereitstellung von Wissen, Suche und Analyse auf den Markt. Dem Anbieter zufolge soll sie die Vorteile eines Enterprise-Content Managementsystems mit semantischer Intelligenz vereinen. Die Wissensvermittlung findet in bestehende Portallösungen und Anwendungen, integriert in der Arbeitsumgebung des Nutzers, statt. Die Interessenschwerpunkte kann der Anwender selbst definieren. Das System analysiert aber auch das Verhalten anhand der durchgeführten Suchanfragen sowie der vom Nutzer verwendeten Dokumente.

Corinna soll alle für einen Anwendungsfall entscheidungsrelevanten Informationen aus den Unternehmenssystemen möglichst effizient zur Verfügung stellen. Die Software besteht aus einem Kern und mehreren als Services konzipierten Modulen, die verschiedene Funktionen und Workflows umfassen. Xtraclass etwa ordnet Dokumente verschiedenen Strukturen zu und lernt anhand vorgegebener Beispiele. Semantics dient der Abbildung von Wissensbeziehungen über Ontologien, Searchminder hilft bei der Suche auch mit Fuzzy Logic, während Duplicate Recognition Dubletten erkennt. Für Dokumente, für die es noch keine Struktur gibt, soll Clustering künftige Zuordnungen vorschlagen. In einem zentralen Wissensspeicher legt die Software mit NLP-Methoden (Natural Language Processing) extrahierte Informationsteile als Ontologien ab. *Susanne Franke*

KURZ NOTIERT



PHP-Entwicklung: Codegear hat die Version 2.0 von Delphi für PHP fertiggestellt. Die IDE enthält eine Visual Component Library, die bekannte PHP-Pakete wie das Zend Framework unterstützt. Außerdem können Entwickler per Drag & Drop mit einer Reihe von DBMS arbeiten: von MySQL bis zum SQL Server, von PostgreSQL bis zu Oracle und DB2. Bis Juni dieses Jahres soll der Preis 178 € betragen, für ein Upgrade 130 € (www.codegear.com).

Content Management: Coremedia, Hamburger CMS-Anbieter, hat in seiner 2008er-Release Erweiterungen für „social Software“, ein Starterkit sowie ein Analysewerkzeug integriert. Bei Ersterer handelt es sich um eine Umgebung für Web-2.0-Anwendungen, das Starterkit bietet fertige Templates sowie Stylesheets und Letzteres erlaubt mit Standardreports, die Nutzung der eigenen Websites zu analysieren (www.coremedia.com).

Kartenformat KML: Google hat im April die XML-Anwendung KML an das Open Geospatioal Consortium (OGC) übergeben, wo die Geodatensprache jetzt als offener Standard betrieben wird (www.opengeospatial.org/standards/kml). Vom OGC stammt außerdem die Geography Markup Language (GML).

Ubuntu 8.04 LTS

Vogelkunde

Markus Franz

Fast zwei Jahre sind seit der Veröffentlichung der letzten Ubuntu-Version (6.06, Codename: Dapper Drake) mit Long Term Support vergangen. Zwar bietet die neue Release viele Neuerungen, nur fallen die im Vergleich zum Vorgänger mäßiger aus.

Mark Shuttleworth, Gründer der Firma Canonical, hat das neue Ubuntu 8.04 als die wichtigste Release der letzten Jahre bezeichnet, da der Debian-Abkömmling inzwischen auf Millionen Computern zum Einsatz kommt. Beim neuen Ubuntu handelt es sich nach fast zwei Jahren wieder um eine LTS-Version (Long Term Support). Das bedeutet, dass Canonical für den Desktop drei und für den Server fünf Jahre lang Updates bereitstellt. Gleichzeitig bietet die Firma in diesem Zeitraum kommerzielle Unterstützung an. Kunden mit Support-Vertrag kommen mit Landscape in den Genuss einer kommerziellen, per Weboberfläche bedienbaren Systemverwaltung. Von der gemeinsamen Administration, über die Softwareverteilung bis zur automatischen Inventarliste kann Landscape den Administrationsaufwand erheblich verringern. Das alles macht die Version 8.04 auch für den Unternehmenseinsatz attraktiv. Sie trägt den Codenamen Hardy Heron und steht als Desktop- und Server-Variante seit dem 24. April zum Download bereit.

Live-CD als Installationsmedium

Wie immer besteht Ubuntu aus einer x86- oder x86_64-Live-CD oder -DVD, die sich auf die Festplatte installieren lässt. Die Varianten für PowerPC und SPARC gehören nicht mehr zum Hauptprojekt, und wurden ausgelagert (ports.ubuntu.com): Ein Update erfordert auf diesen Plattformen das Anpassen der Paketquellen. Darüber hinaus gibt es eine spezielle Server-Installations-CD ohne GUI. Weiter existieren die ebenfalls aktualisierten Variationen wie Kubuntu, Xubuntu oder Edubuntu. Von diesen schmückt nur Edubuntu das Prädikat LTS – bei Kubuntu stand dem wohl die anstehende Migration von KDE 3.5.x auf KDE 4 entgegen.

Für Umsteiger ist das Installations-Tool namens Wubi gedacht. Es läuft unter Windows und installiert Ubuntu ins Windows-Dateisystem – man kann aber trotzdem wie gewohnt beim Hochfahren Ubuntu als Betriebssystem auswählen. Benutzern erspart Wubi so nicht nur das gefährliche Partitionieren, sondern Ubuntu lässt sich bei Nichtgefallen auch schnell und restlos wieder entfernen. Hierbei hilft ein neuer Assistent.

Als Standard-Desktop setzt Ubuntu auch in der neuen Version auf Gnome 2.22. Die aktualisierte Auflage verwendet statt GnomeVFS nun das virtuelle Dateisystem GVFS, das den Dateimanager Nautilus spürbar beschleunigt. Außerdem lassen sich damit Partitionen über FUSE (File System in User Space) einbinden und der direkte Zugriff auf FTP, SMB, DAV und andere realisieren. Das neue Gnome bringt den verbesserten Videoplayer Totem mit, der nun deutlich mehr Formate abspielt. Weiter fällt auf, dass die Entwickler den alten VNC-Client durch das komfortable Pendant Vinagre ersetzten: Damit lassen sich automatisch zur Fernsteuerung freigegebene Rechner im Netz finden.

Ebenfalls neu ist Firefox 3 – obwohl erst als Beta vorliegend, hat der Browser es in die LTS-Release geschafft. Canonical begründet dies mit der langen Laufzeit von Hardy Heron, zu der die Vorversion von Firefox am besten passt. Ob die Stabilität Firmenansprüchen genügt, muss sich erst zeigen. Der neue Firefox fällt beim Aufbau komplexer Webseiten angenehm auf – hier sind die neue Rendering-Engine und die Javascript-Implementierung deutlich schneller als in den Vorversionen. Der Lesezeichen-Manager präsentiert sich komfortabler und macht Spaß: Er bietet nicht nur die Standard-Lesezeichen, sondern auch dynamisch generierte wie die zuletzt besuchten oder am häufigsten verwendeten Seiten. Umständlicher ist aber die Warnung bei verschlüsselten Seiten mit nicht absolut sicherem Zertifikat: Dann muss man sich durch drei Menüs klicken, um den Zugang manuell zu genehmigen – bisher ging das schneller.

Audio-CDs und andere Medien lassen sich mit Ubuntu 8.04 sowohl direkt in Nautilus als auch im neuen Brasero Disc Burning erstellen. Erfreulich ist dabei die einfache Möglichkeit, schnell ein Medium von einer Image-Datei zu brennen. Kleinere Änderungen am Desktop runden das Bild positiv ab: Neben einem Bittorrent-Client bietet Ubuntu nun in der Standardkonfiguration auch einen ausgewachsenen Download-Manager. Openoffice hat in Version 2.4 Einzug in Ubuntu gehalten.

Ein Blick unter die Haube

Im Hintergrund von Ubuntu werkelt der Kernel 2.6.24-3. Ebenso wie der Vorgänger bringt dieser den Fair-Scheduler mit, der die Rechenzeit gerechter auf die Anwendungen verteilt. Er soll in der aktuellen Release ein angenehmes Arbeiten mit Multimedia und der Textverarbeitung gewährleisten. Als Sound-Server setzt Ubuntu nun Pulse Audio ein: Damit lassen sich mehrere Ausgabequellen besser mixen sowie der Sound auf einer anderen Maschine im Netz ausgeben. Um die Darstellung des GUI kümmert sich Xorg 7.3, das die automatische Konfiguration vereinfacht: Im laufenden Betrieb lässt sich nun die Größe des Bildschirm ebenso ändern wie seine Drehung. Notebook-Nutzern dürfte gefallen, dass sich damit auch externe Monitore oder Beamer dynamisch ins System einbinden lassen. Für 3D-Effekte aktualisierten die Entwickler Compiz nebst zugehöriger Plug-ins.

In der Server-Ausgabe verzichtet Hardy Heron restlos auf X, was der Systemsicherheit zugutekommt. Apropos Sicherheit: Wie bisher integriert Ubuntu AppArmor. Es existieren nun aber für mehr Anwendungen vordefinierte Richtlinien, sodass man diese schnell einsetzen kann. SELinux steht im Universe-Repository zur Verfügung, Canonical bietet allerdings im Rahmen des Long Term Support keine Unterstützung dafür. Das von Fedora bekannte Policy-Kit schafft Sicherheit, indem man Benutzern gezielt Rechte für Verwaltungsaufgaben zuweisen kann. Die UFW (Uncomplicated Firewall) komplettiert das Sicherheitskonzept: Das Kommandozeilenprogramm für Iptables richtet eine auf Netfilter basierende Firewall schnell ein – eine grafische Oberfläche wäre jedoch wünschenswert gewesen.

Als Virtualisierungslösung dient im neuen Ubuntu nun KVM. Mit Red Hats Virt Manager gestaltet sich die Kontrolle über virtuelle Maschinen einfacher als bisher. Im Netzwerk gefällt die Software Likewise Open, die für Authentifizierung im Active Directory zuständig ist. Mit OpenJDK 6 enthält Ubuntu nun auch ein komplett freies Java, mit dem sich Eclipse problemlos ausführen lässt.

Mit Ubuntu 8.04 (Hardy Heron) hat Canonical wirklich eine leistungsfähige Linux-Distribution vorgestellt. Bis auf Firefox, dessen Beta-Status einfach nicht zu einer LTS-Release passen mag, gibt die neue Version in den Punkten Sicherheit, Programme und Stabilität ein gewohnt gutes Bild ab. (avr)

iX-Link ix0806032

Daten und Preise

Produktname: Ubuntu 8.04 LTS
Anbieter: Canonical Ltd.
Download: www.ubuntu.com/download
Support: ab 170 €/600 € pro Jahr (Desktop Server)
Details: www.canonical.com/services/support

Hans Reiser des Mordes an seiner Frau schuldig gesprochen

Seit November 2007 muss sich der bekannte Entwickler Hans Reiser für das Verschwinden seiner Frau verantworten. Der Initiator der Journaling-Dateisysteme ReiserFS und Reiser4 soll seine Frau getötet haben. Am 28. April haben ihn die Geschworenen eines Bezirksgerichts nach nur drei Tagen Beratung schuldig gesprochen.

Der Fall erregte gerade in der Community große Aufmerksamkeit. Während des fünfmonatigen Verfahrens konnte sich die Anklage nur auf Indizien stützen. Weder wurde die Leiche von Reisers Frau gefunden noch gibt es Zeugen der Tat. Nina und Hans Reiser lernten einander 1998 in Russland kennen, heirateten kurz danach und zogen an die US-Westküste. Das Ehepaar hat zwei Kinder, jedoch reichte Nina Reiser 2004 die Scheidung ein. Ein erbitterter Scheidungskrieg begann.

Im September 2006 verschwand Nina Reiser spurlos, nachdem sie ihre Kinder bei Hans Reiser abgegeben hatte. Einige Tage später wurde ihr Auto unweit ihrer Wohnung mit verdorbenen Lebensmitteln darin gefunden. Im Laufe des Verfahrens kamen über 60 Zeugen zu Wort. Es nahm jedoch eine dramatische Wendung, als Hans Reiser in den Zeugenstand trat, um sein auffälliges Verhalten nach dem Verschwinden seiner Frau zu erklären. Als er gefragt wurde, warum der Beifahrersitz seines Zweisitzers fehlt, gab er zur Antwort, dass er in dem Auto schlafe und mehr Platz brauche. Als die Polizei jedoch den Wagen beschlagnahmte, stand im Inneren mehrere Zentimeter hoch das Wasser. Reiser hatte offensichtlich versucht, den Wagen gründlich zu reinigen. Dass in seinem Besitz ein Buch mit dem Titel „Der perfekte Mord“ gefunden wurde, kommentierte er mit der Erklärung, er habe die Vorgehensweise der Polizei besser verstehen wollen, nachdem er im Fadenkreuz der Ermittler stand.

Hans Reiser verstärkte durch seine Aussage nur die Anschuldigungen gegen ihn. Er behauptete im Verfahren immer wieder, Nina sei heimlich in ihre Heimat zurückgekehrt. Andere Zeugen präsentierten jedoch ein anderes Bild von der Vermissten. Nina Reiser würde nie ihre Kinder im Stich lassen und ohne sie das Land verlassen.

Die Geschworenen gaben nun dem Staatsanwalt recht. Die Verkündung des Strafmaßes ist für den 9. Juli angesetzt. Reiser muss mit 25 Jahren Gefängnis rechnen. Reisers Verteidiger hatte auf Freispruch plädiert. Er gab zwar zu, sein Mandant sei ein äußerst schwieriger und oft despotischer Mensch, aber das mache ihn nicht zum Mörder.

Auf die Zukunft von Linux und Reiser4 dürfte die Verurteilung keinen Einfluss mehr haben. Zwar ist die bislang hinter der ReiserFS- und Reiser4-Entwicklung stehende Firma Namesys seit einigen Monaten nicht mehr operativ tätig, jedoch entwickeln einige vormalige Namesys-Mitarbeiter Reiser4 in Eigeninitiative weiter. Suse und Debian setzten bisher beide Reiser3 ein – beide wollen zukünftig auf Ext3 sowie dessen Nachfolger Ext4 setzen.

Arno Puder

Bitkom-Leitfaden zur Patentanmeldung

Im „Leitfaden zur Patentierung computerimplementierter Erfindungen“ beschreibt der Branchenverband Bitkom, welche Kriterien Unternehmen bei Patentanträgen von IT-Systemen und technisch einsetzbaren Computerprogrammen berücksichtigen sollten. Der Leitfaden soll vor allem kleine und mittlere Unternehmen unterstützen. Nach Auffassung des Branchenverbands können sie ihre Erfindungen nur mithilfe von Patenten vor Imitationen schützen. Darüber hinaus seien Patente der einzig wirksame Schutz vor dem Verlust des geistigen Eigentums an die Konkurrenz. Außerdem stärken Patente die Position der KMU gegenüber Großunternehmen und erhöhen den Wert eines Unternehmens. So können sie zum Beispiel als Tauschwährung bei Geschäftsverhandlungen eingesetzt werden. Nach Angaben von Bitkom erfüllen viele Patentanmeldungen die Kriterien der Patentämter nicht. Das führt dazu, dass die Ämter im Jahr 2007 weniger Patente zugelassen haben als im Vorjahr: In Europa sank die Zahl der Zulassungen um 13 Prozent, in Deutschland um 16 Prozent. Der Leitfaden informiert über den aktuellen rechtlichen Stand von Softwarepatenten, über die Anmeldeprozedur im nationalen und internationalen Umfeld sowie über Kosten und Zeitaufwand und demonstriert anhand eines Beispiels, in welcher Form der Antragsteller seine Erfindung beschreiben sollte. Der kostenlose Leitfaden ist im Internet als PDF verfügbar, siehe *iX*-Link. *Barbara Lange*

iX-Link ix0806034



Vor allem kleine und mittlere Unternehmen will der Branchenverband Bitkom mit seiner kostenlosen Patentbroschüre unterstützen.

Vollständige Datenverschlüsselung

Der Mobile Guardian Enterprise Edition 6.0 von Credant lässt sich in Symantecs Managementplattform Altiris für Endgeräte integrieren. Damit sollen IT-Administratoren die Möglichkeit erhalten, über die Verwaltungskonsole Daten auf mobilen Endgeräten eines Unternehmens zu verschlüsseln und zu auditieren. Das Produkt soll alle Daten unabhängig von ihrem Speicherort und für den Endbenutzer transparent verschlüsseln – ob auf dem Desktop, einem mobilen Endgerät oder auf externen Speichermedien wie USB-Sticks. Administratoren können die Software zentral verwalten und Policies aufsetzen, die der Guardian an Shield-Agenten auf den Desktops beziehungsweise Laptops oder PDAs schickt, und die festlegen, was und wie verschlüsselt wird.

Dateien und Ordner lassen sich entweder so verschlüsseln, dass jeder in der Organisation sie öffnen kann, oder so, dass nur der jeweilige Nutzer sie verwenden kann. Mobile Speichermedien, die zum ersten Mal versuchen, sich mit dem Unternehmensnetzwerk zu verbinden, werden automatisch erkannt und in die Sicherheitsvorkehrungen eingebunden. Hinzugekommen ist in der neuen Version ein Stand-alone Windows Shield für Daten auf Maschinen, die nicht zentral verwaltet werden, etwa die eines Subunternehmers oder Geschäftspartners. *Susanne Franke*

Studie warnt vor Schlamperei bei IAM

Kuppinger, Cole + Partner haben zwei neue Studien durchgeführt. Die eine untersucht Single-Sign-On (SSO) als eines der wichtigsten Felder im Identity- und Access-Management (IAM). Durch eine vereinheitlichte Authentifizierung können unter anderem die Risiken für Sicherheit und Compliance sowie Help-Desk-Kosten reduziert werden. Innerhalb der Vielzahl der technischen Ansätze für das SSO erachten die Experten Identity Federation (unternehmensübergreifendes ID-Management) und ergänzend das benutzerzentrierte Identity-Management (Kontrolle des Nutzers über seine Daten) als günstigste Ansätze, weil sie sich auf alle Anwendungsfelder sowohl mit internen als auch externen Benutzern und im heterogenen Umfeld flexibel einsetzen lassen. Da Federation aber erst langsam kommt, werden auch auf lange Sicht ergänzende Verfahren benötigt. Die größte Bedeutung haben dabei Enterprise-Single-Sign-On-Lösungen sowie verwaltete Verfahren für lokales SSO in Verbindung mit Token für die internen Benutzer und das Web-SSO für externe Benutzergruppen, aber auch interne Webportale. Ein weiterer Report des Hauses untersucht das Verhältnis von IAM und serviceorientierte Architekturen. Die Studie macht deutlich, dass nur die wenigsten Unternehmen ein „definiertes Zusammenspiel“ zwischen den beiden Bereichen haben. Kuppinger warnt vor den Konsequenzen der fehlenden Governance für die Compliance und das Risikomanagement. Die Studien (195 € bzw. 295 €) sind über die Website www.kuppingercole.com zu bestellen. *Susanne Franke*


iX-Link ix0806034

RFID-Enttäuschung bei Handel und Industrie

Für die Studie „RFID – Spielwiese für Technologiebegeisterte oder Schlüsseltechnologie zur Effizienzsteigerung von Geschäftsprozessen?“ interviewte das Fraunhofer-Institut für Produktionstechnologie IPT und die P3 Ingenieurgesellschaft mbH Vertreter von 1000 Unternehmen aus den Bereichen Logistik, Maschinenbau, Automobilbau, Elektrotechnik sowie Luft- und Raumfahrt. Gleichzeitig testeten die beteiligten Autoren die Leistungsfähigkeit der verschiedensten RFID-Systeme unter Laborbedingungen.

Die Ergebnisse: 80 Prozent der Befragten bezeichneten ihre Erwartungen und Erfahrungen mit RFID als negativ. Pilotprojekte sind teuer, führen aber vielfach nicht zu den erhofften Ergebnissen. Zwar nannten 72 Prozent der Unternehmen die Automatisierung gesamter Prozessketten als Ziel ihrer RFID-Einführung, kamen jedoch über einfache logistische Anwendungen nicht hinaus, da sie wertschöpfende Unternehmen gar nicht einbezogen hatten. RFID ermöglicht zwar eine Integration unternehmensübergreifender Prozesse, aber nur 66 Prozent der befragten Unternehmen haben dieses in ihren RFID-Projekten auch realisiert.

Darüber hinaus fehlte es an Wirtschaftlichkeitsbetrachtungen. Fast 25 Prozent der Befragten hatten diesen Schritt im Vorfeld eines Projektes übersprungen. Damit konnten sie ein wichtiges Ziel, Kostensenkung durch RFID, häufig nicht erreichen. 30 Prozent hatten auch keine technischen Machbarkeitsstudien durchgeführt – ein weiterer Mangel, da RFID-Systeme in jedem Unternehmensumfeld auf eigene Bedingungen treffen. Die Studie bemängelt die Inkompatibilität existierender Standards und technische Schwierigkeiten beim Auslesen von Daten bei Ultra-Hochfrequenz-Systemen.

Fazit: Immer noch sind es die Technologiebegeisterten, die RFID einsetzen. Damit Unternehmen die Mängel in den Griff bekommen, werden sie immer häufiger Dienstleister beauftragen müssen. Die Studie kostet 199 Euro und kann über Mario Isermann (Fraunhofer IPT, siehe *iX*-Link) bezogen werden. *Barbara Lange*

iX-Link ix0806034

Microsoft verwaltet jetzt auch Linux

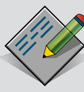
Auf dem „Management Summit 2008“ in Las Vegas hat Microsoft neue Funktionen rund um die System-Center-Familie vorgestellt. Besondere Aufmerksamkeit genoss die Beta-Version der Cross Platform Extensions für den System Center Operations Manager 2007.

Sie erlauben der Managementumgebung, neben den eigenen Windows-Servern auch Fremdplattformen in die Verwaltung einzubinden. „Out of the box“ gilt das für Server unter HP-UX, Red Hat Enterprise Linux, Sun Solaris und Suse Linux. Weitere System- und Anwendungsunterstützung sollen Partnerfirmen beisteuern. So haben bereits Novell, Quest und Xandros eigene Add-ons zu den Cross Platform Extensions angekündigt.

Basis der Cross Platform Extensions sind unter anderem WS-Management und Open Pegasus. Letzteres ist eine Open-Source-Variante der DMTF-Spezifikationen CIM (Common Information Model) und WBEM (Web Based Enterprise Management). Nach einem Objekt-Provider-Modell werden dabei die Informationen der zu verwaltenden Objekte über den CIMOM (Model Object Modeller) für die eigentlichen Managementanwendungen „übersetzt“. Microsoft kündigte an, dem Open Pegasus Steering Committee beizutreten und dort eigene Programmquellen einzubringen. Dies soll unter dem Dach der Microsoft Public License geschehen, die von der Open Source Initiative (OSI) anerkannt ist.

Neben der breiteren Plattformunterstützung hat Microsoft sein System Center auch mit Blick auf die Verwaltung virtualisierter Umgebungen ausgebaut. Vorgestellt wurde unter anderem der neue Virtual Machine Manager, mit dem sich virtuelle Maschinen konfigurieren und verteilen lassen. Dabei findet neben den eigenen Produkten Windows Server 2008 Hyper-V und Virtual Server 2005 R2 auch VMwares ESX Server Unterstützung. Zu guter Letzt waren in Las Vegas Beta-Versionen neuer Konnektoren zu sehen, mit denen sich der System Center Operations Manager mit anderen Managementumgebungen „versteht“, etwa IBM Tivoli oder HPs Openview. *Achim Born*

KURZ NOTIERT



Geschluckt: Nimsoft hat Indicative Software gekauft und erweitert damit sein Portfolio um Komponenten für Business Service Management (BSM) und um Funktionen für die Überwachung von Antwortzeiten. Die Indicative-Tools bieten unter anderem Funktionen zur Service-Modellierung, zum Echtzeit-Monitoring benutzerseitiger Antwortzeiten sowie zur Analyse von J2EE- und .NET-Anwendungen.

Eingebaut: BMC integriert Tibcos SOA-Plattform Activematrix in das eigene Business Service Management (BSM) mit dem Ziel, heterogene serviceorientierte Architekturen besser zu verwalten. Das Ergebnis ist die Kombination der Managementangebote von BMC mit den Tibco-Funktionen für Service-Integration, Entwicklung zusammengesetzter Anwendungen und Governance.

Alles im Blick: Numara Software hat im Rahmen der diesjährigen Komcom Süd in Karlsruhe eine neue Ausgabe von Numara Track-It vorgestellt. Die Version 8.1 der Inventar- und Lizenzmanagementsoftware hat eine neu gestaltete Benutzeroberfläche, soll sich flexibel an die spezifischen IT-Anforderungen im öffentlichen Dienst anpassen lassen und kann nun Strichcodes verarbeiten.

XML-Software: Mit ihrer zweiten Version der 2008er-XML-Suite bewältigt der Editor XMLSpy von Altova deutlich umfangreichere XML-Dokumente. Außerdem unterstützt er Visual Studio 2008 und verfügt über erweiterte XSLT- und XQuery-Eigenschaften.

Breko-Verband kritisiert Bundesnetzagentur wegen zu hoher Leistungsmiete

Die Geschäfte laufen im Grunde nicht schlecht für die im Bundesverband Breitbandkommunikation Breko zusammengeschlossenen Netzbetreiber. Im vergangenen Geschäftsjahr erzielten sie einen Umsatz von 5,6 Mrd. Euro und damit bereinigt um Firmenzugänge ein Plus gegenüber dem Vorjahr um 20 %. Im laufenden Jahr wollen die Breko-Mitglieder, die 99 % des Festnetzwettbewerbs der Telekom repräsentieren, die 6-Milliarden-Grenze packen.

Bei der Vorstellung der Jahresbilanz gab Breko-Präsident Peer Knauer, im Hauptberuf Versatel-Chef, jedoch zu bedenken: „Diesen Erfolg haben wir eher trotz als wegen der Regulierungsvorgaben erreicht. Die Miete der Teilnehmeranschlussleitung ist mit 10,50 Euro im europäischen Vergleich immer noch zu hoch und wir subventionieren immer noch mit rund 2 Milliarden Euro Terminierungsentgelten pro Jahr die Preisgestaltung der Mobilfunker.“

Unzufrieden zeigte sich der Verbandspräsident insbesondere mit der Länge der Verfahren bei der Bundesnetzagentur. Es gehe nicht an, so Knauer, dass sich beispielsweise die Beratungen über den Standardvertrag zur Teilnehmeranschlussleitung über zwei Jahre hingezogen hätten und entscheidende Missbrauchsverfahren nicht stringent genug angegangen würden. Nicht hinnehmbar seien auch Entscheidungen, die eine weitere Entwertung der vorhandenen und zu schaffenden TK-Infrastruktur herbeiführen und das Konsistenzgebot unterlaufen würden. Insbesondere bei der Festlegung des Entgeltes für den IP-Bitstrom-Zugang am 13. Mai fordert der Verbandschef ein klares Signal für den Werterhalt von TK-Infrastruktur. Knauer: „Ein zu niedriges Bitstrom-Entgelt würde ein weiteres Mal die Reseller bevorzugen, die kaum eigene Infrastruktur besitzen und ihre Dienste einfach Huckepack auf den Netzen anderer transportieren. Das muss seinen Preis haben.“

Mit anderen Worten: Anders als der Reseller United Internet (1&1) hoffen die Breko-Firmen auf ein hohes Entgelt. In Hintergrundgesprächen ging es um eine Gebühr von 22,23 Euro, die weiterhin Investitionen in eigene Infrastruktur (Straße aufreißen und Kabel verlegen) rechtfertigen würden. Stimmen die Voraussetzungen, erwartet der Verband ein Wachstum der DSL-Anschlusszahlen bei den Mitgliedern von 6,1 Mio. auf 7,5 Mio. im laufenden Jahr. Derzeit stellen die Firmen etwa ein Drittel der rund 20 Mio. DSL-Anschlüsse in Deutschland. 1,1 Mrd. Euro wollen die Unternehmen 2008 in den weiteren Netzausbau stecken und damit – gemessen am Marktanteil – viermal so viel wie die Telekom. Fast drei Viertel (74 %) planen, das eigene Glasfasernetz bis an die Haushalte heranzuführen („Fiber to the Home“). Dies sei allerdings nur dann sinnvoll, wenn ein geeigneter Weg unter Einbeziehung der jetzigen Netzstruktur mit den Telekom-Hauptverteilern gefunden würde.

Dass eigene Leitungen auch künftig wettbewerbsrelevant sind, steht für Knauer außer Frage. Durch langsameres Kundenwachstum, steigende Marketingkosten sowie sinkende Preise werde eine Marktbereinigung immer wahrscheinlicher. Deshalb sei die schiere Bandbreite entscheidend für Erfolg oder Misserfolg im DSL-Geschäft.

KURZ NOTIERT

Aufkauf: Cisco beabsichtigt alle Anteile an Nuova Systems zu erwerben. Das in San Jose ansässige und auf Rechenzentren spezialisierte Startup-Unternehmen agiert bereits seit Mitte 2006 als 80-prozentige Tochter der Netzequipment-Firma mit dem Ergebnis der Switching-Plattform Nexus 5000.

Eingekauft: Keynote Systems plant, die kleine französische Softwareschmiede Zandan zu übernehmen, um sich die exklusiven Rechte an der für die Mobile Application Perspective (MAP) genutzten Technik zu sichern. Bislang bestand nur ein nicht exklusiver OEM-Vertrag.

Vermessen: Der eco-Verband, mit eigenen Zertifizierungen für Rechenzentren bereits am Markt aktiv, plant die Entwicklung eines Effizienz-Benchmark für hiesige RZ. Hierzu initiierte eco nun im Vorfeld eine bis Ende Mai laufende Datenerhebungsphase.

Datenschutz-Hausaufgaben für StudiVZ & Co.

Die obersten Aufsichtsbehörden für den Datenschutz in der Wirtschaft haben erstmals Leitlinien für Betreiber von sozialen Netzwerken sowie von Bewertungsportalen veröffentlicht (siehe *iX*-Link). Portale wie SchuelerVZ oder StudiVZ müssen laut dem Ende April veröffentlichten Beschluss ihre Nutzer umfassend über die Verarbeitung ihrer Daten informieren. Auch die Entscheidung, wer welche Daten sehen darf, liegt beim Nutzer. Die Speicherung seiner Daten auf Vorrat hingegen oder personalisierte Werbung muss er nicht hinnehmen. Profil und Bild müssen jederzeit vom Nutzer löschbar sein, außerdem hat er das Recht auf Benutzung eines Pseudonyms in solchen Netzwerken.

Rechtlich komplizierter verhält es sich bei Bewertungsportalen wie spickmich.de und meinprof.de, das verraten die allgemein gehaltenen Formulierungen des zweiten Beschlusses: Hier weisen die Datenschutzaufsichtsbehörden darauf hin, dass es sich bei den auf solchen Portalen allen zugänglichen Informationen um sensible Informationen und subjektive Werturteile handelt. Betreiber müssen die Vorgaben des Bundesdatenschutzgesetzes über die geschäftsmäßige Verarbeitung personenbezogener Daten einhalten und dürfen nicht die freie Meinungsäußerung über das Recht auf informationelle Selbstbestimmung stellen.

Was hinter diesen im Vergleich zum ersten Beschluss sehr unkonkreten Formulierungen steckt, erläutert Thomas Petri, stellvertretender Berliner Beauftragter für Datenschutz und Informationssicherheit. Bewertungsportale werden von vielen Datenschützern als Onlineauskunfteien betrachtet. Das bedeutet: Wenn für sie keine Spezialregelung gilt, ist Paragraf 29 des Bundesdatenschutzgesetzes auf sie anzuwenden. Dieser legt jedoch fest, dass Informationen über Personen nur dann zugänglich sein dürfen, wenn der Abrufende ein berechtigtes Interesse glaubhaft machen kann. Nach Ansicht der Berliner Datenschützer sind daher solche Portale, die die Informationen für jeden zugänglich machen, nicht rechtens.

Es geht noch weiter: Nicht nur der Nachweis des berechtigten Interesses fehlt, auch müsste die verantwortliche Stelle – in dem Fall der Portalbetreiber – diese Nachweise dokumentieren. Außerdem, so Petri, könne es nicht sein, dass die betroffenen Personen nicht informiert würden. Man könne schließlich nicht sämtliche Bewertungsportale durchsuchen, ob irgendetwas dort über einen selbst veröffentlicht sei. Auch hier sind seiner Ansicht nach die Betreiber in der Pflicht, die Betroffenen zu informieren. Darüber hinaus haben sie darauf zu achten, dass die bewerteten Personen nicht unangemessen beschimpft werden. Denn, und hier findet man sich wieder beim letzten Punkt des Beschlusses, die freie Meinungsäußerung kann keinen höheren Stellenwert haben als das Persönlichkeitsrecht des Bewerteten.

Die Berliner Datenschützer haben es sich zur Aufgabe gemacht, Portalbetreiber nachdrücklich auf die Erfüllung datenschutzrechtlicher Anforderungen hinzuweisen – notfalls mit Konsequenzen. Derzeit, so Petri, habe man gegen einen Portalbetreiber bereits einen Bußgeldbescheid verhängt.

Ute Roos

iX-Link ix0806036

PLATON von T-Systems und Microsoft soll Datenaustausch sichern

„Platform for Orchestrated Engineering Networks“ oder kurz PLATON heißt das von T-Systems und Microsoft gemeinsam entwickelte Produkt zum sicheren Datenaustausch. Kernstück der Software ist ein „Secure Data Container“ (SDC), der auf dem Open-Packaging-Convention-Format des Open-XML-Standards beruht.

In ihn lassen sich verschiedene Datenformate hineinkopieren, etwa Stücklistentabellen, 3D-CAD-Modelle, Programmcode et cetera. Zusätzlich erhält jedes in einer Container-Datei gespeicherte Objekt eine Zugriffsrechteliste für den Empfänger. Alle Elemente werden per IBE (Identity Based Encryption) verschlüsselt. PLATON weist jedem solchermaßen gesicherten Container eine eindeutige Identifikationsnummer und einen Lieferschein zu.

Nach Aussagen von Microsoft würde bei einem Verlust eines Containers dessen Entschlüsselung nach heutigen Stand der Technik acht bis zehn Jahre dauern.

Empfängerseitig benötigt der Anwender die PLATON-Clientsoftware, einen USB-Stick mit seiner Signatur und einen Internetzugang. Der Client meldet die Ankunft einer Datensendung, authentifiziert via Rights Management den Empfänger und zeigt ihm den Lieferschein, also welche Inhalte der Container enthält. Außerdem startet er die für das Öffnen erforderliche Anwendung, gegebenenfalls mit den durch den Versender eingeschränkten Rechten – etwa nur Lese- und kein Speicherrecht. Der Absender benutzt seinerseits die Clientsoftware – mit entsprechender Anbindung an ein Quellsystem –, um Zugriffsrechte zu definieren sowie Encryption-Keys, Versandart und weitere Details festzulegen.

IBM betreibt IT von ProSiebenSat.1

Unter Dach und Fach ist nach langem Ringen zumindest ein Teilverkauf der ProSiebenSat.1 Produktion (PSP), einer Tochterfirma der ProSiebenSat.1 Media AG. Künftig wird IBM für die Fernsehsenderfamilie die IT betreiben. Hierzu schlossen beide Firmen einen Outsourcing-Vertrag über zehn Jahre mit einem Volumen von über 200 Mio. Euro. Konkret übernimmt IBM die Verantwortung für die Planung, den technischen Support sowie für die Bereitstellung der Anwendungen, Internettechnik und IT-Infrastrukturen für die Sendergruppe. Zudem soll der IT-Konzern die Kern-Geschäftsanwendungen, darunter Werbezeitenvermarktung, Programmplanung und das Rechtemanagement, modernisieren sowie über alle Distributionskanäle integrieren und verzahnen.

Damit verknüpft ist der Wunsch von ProSiebenSat.1, künftig flexibler und schneller arbeiten zu können bei gleichzeitiger Kostensenkung. Außerdem soll eine „paneuropäische“ Digitalplattform einschließlich zentraler Playout-Zentren entstehen, eine komplett digitale, bandlose Infrastruktur.

PAN Manager für FSCs BX600-Blades

Als neue Umgebung für die zentrale Administration seiner Blade-Server BX600 liefert Fujitsu Siemens Computers (FSC) den PAN Manager. Er gehörte bisher als fester Bestandteil ausschließlich zu den in Hardware virtualisierten Bladeframe-Systemen von Egenera und erlaubt zudem die Virtualisierung auf Basis von Xen. Der Administrator kann damit sowohl physische als auch virtuelle Server einrichten, überwachen und fernsteuern, Cluster sowie HAV-Systeme aufbauen und ein Disaster Recovery durchführen. FSC vertreibt die Bladeframes als OEM in EMEA exklusiv.

Mit dem PAN Manager will FSC den Grundstein für seine Flexframe Infrastructure legen und eine Alternative zu VMware Infrastructure 3 bieten. Es geht vor allem darum, für die zentrale Administration von Servern eine einheitliche Sicht zu schaffen und so den Aufwand für Schulung, Einarbeitung und zusätzliche Software zu verringern. Egenera hatte bereits im November 2007 angekündigt, den PAN Manager auch für zertifizierte Systeme anderer Hersteller anbieten zu wollen. Im März dieses Jahres hat Dell dazu eine Partnerschaft mit Egenera geschlossen.



OpenBSD 4.3 freigegeben

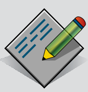
Mit neuen Versionen der vorwiegend klassischen Software geht OpenBSD 4.3 ins Rennen. Die Distribution gibt es zum freien Download als ISO-Image. Mit der neuen Version sind weitere Hardwarearchitekturen hinzugekommen: SMP-Support für Sparc64, HPs PA-RISC im 32-Bit-Mode für die K-Class-Server (hppa), SMP auf Motorolas 881x0-Prozessoren (mvme88k) und weitere Treiber für SGIs Systeme mit Mips-CPUs wie die O2-Workstation.

Über 30 neue Treiber erweitern die Unterstützung für eine Vielzahl teils exotischer Hardwarekomponenten. Bei der Software stehen neben einer großen Zahl von Tools vor allem neue Versionen von Anwendungen im Vordergrund, darunter Gnome 2.20.3, KDE 3.5.8 sowie Xfce 4.4.2, GNUstep 1.14.2, Openmotif 2.3.0, MySQL 5.0.51a, PostgreSQL 8.2.6 und Openoffice 2.3.1.

Wie bisher kann man OpenBSD 4.3 auf CD bestellen, womit das Projekt versucht, einen Teil seiner Kosten zu decken.



KURZ NOTIERT



Weitergehen: Mit Virtualbox 1.6 können Anwender nun auch virtuelle Rechner auf Mac OS X und Solaris erzeugen. Linux- und Solaris-Gäste können in einem Fenster auf dem Host-Desktop im Seamless Windowing Mode laufen, was bisher Windows vorbehalten war (www.virtualbox.org/wiki/Downloads).

Speicherwerk: Zwei neue Entwicklungs-Tools und erweiterten Service bietet Sun für die Speicherverwaltung mit OpenSolaris an. Sie hören auf die sperrigen Namen „Build an OpenSolaris storage server in 10 minutes or less“ und „Simple Steps to building a NAS appliance“. Die Sammlung gibt es unter www.sun.com/openstorage.

Rundendrehen: Unter OpenPowerlink hat die SYS TEC electronic (Greiz) ihren Software-Stack für Ethernet Powerlink als Open Source (BSD-Lizenz) herausgegeben, der Software für den Manage- und die Controller-Nodes enthält. Mit handelsüblichen Onboard-Controllern unter Linux (ab Kernel 2.6.23) sollen damit Zykluszeiten bis herab zu 0,5 ms zu erzielen sein (www.ethernet-powerlink.org).

Solaris 10 5/08 und OpenSolaris frei

Mit der Version 5/08 von Solaris 10 hat Sun Microsystems den Nachfolger der Version vom August 2007 (8/07) per Download frei zur Verfügung gestellt (www.sun.com/software/solaris/get.jsp). Wenige Tage später, zur jährlich stattfindenden Entwickler-Konferenz CommunityOne, folgte die Bereitstellung einer Live-CD von OpenSolaris 2008.5 (Indiana) auf opensolaris.org. Solaris 10 5/08 gibt es als Image-Datei für eine DVD oder sechs CDs auf der Site von Sun zum kostenlosen Download. Alternativ bietet Sun Media-Kits für 35 US-$ an. Bei dem CD-Set gibt es eine Sparc- und eine x86-Version. Die Kits enthalten neben der Entwicklungsumgebung Studio 12, HPC Clustertools 7.1 und Netbeans IDE 6.0.1 eine Sammlung zusätzlicher Software, die Solaris Software Companion.

Sun setzt als Mindestanforderungen 2 GByte Platz auf der Festplatte sowie 128 MByte, für x86er 256 MByte RAM voraus. Außer auf Suns eigenen UltraSparc und FSCs Sparc64 läuft Solaris 10 auf den Prozessoren von AMD, Intel und VIA, sowohl in der 32-, als auch in der 64-Bit-Variante.

Zu den Neuerungen zählen vor allem:
– die Behandlung von Speicherfehlern nun auch für Xeon-, AMD64-, UltraSparc-T1- und -T2-CPUs,
– Suns StorEdge Traffic Manager zur Datenverwaltung,
– Solaris Live Upgrade für Container,
– das Internet Printing Protocol (IPP) auf der Client-Seite, die Open Printing API (PAPI) sowie VNC-Client und -Server,
– Suns Validation Test Suite (SunVTS),
– Unterstützung für UltraSPARC T2 Shared Contexts, Intels CPUID, Intels MONITOR/MWAIT, Infiniband und die Memory Placement Optimization (MPO),
– UltraSparc T2 ECC Acceleration und Solaris Trusted Extensions,
– Powermanagement für die 64-Bit-CPUs von Intel und AMD,
– Flash Player, der Instant Messenger Pidgin, Locale Creator sowie die Eingabemöglichkeit von traditionellen chinesischen Zeichen und
– das Aufteilen der CPU-Ressourcen in sogenannte CPU-Caps bei der Virtualisierung.

OpenSolaris kommt mit einer CD aus, das ISO-Image ist 686 MByte groß. Außerdem kann man die Life-CD kostenfrei bei Sun bestellen. Es handelt sich um ein vollwertiges Desktop-Betriebssystem für x86-Architekturen, das einige Kernfeatures von Solaris10 enthält, unter anderem das Zettabyte File System (ZFS), die Service Management Facility (SMF) sowie den System-Tracer Dtrace. Sun will damit vor allem Linux-Anwender für Solaris gewinnen, die sich mit der Gnome-Oberfläche in einer vertrauten Umgebung wiederfinden. Außerdem sind eine ganze Reihe unter Linux üblicher Anwendungen dabei. Das OpenSolaris-Projekt leitet Ian Murdock, der die Debian-Distribution aus der Taufe hob und nun seit über einem Jahr für Sun arbeitet.

Bei der Free Solaris Express Developer Edition (SXDE), die auf der Site developers.sun.com/sxde/ bereitsteht, handelt es sich um den jeweils neuesten Build aus den Open-Source-Quellen von Solaris.



Überwachung für VMs von Vizioncore

Mit vCharter Pro will Vizioncore seinen Kunden ein Management-System anbieten, mit denen sie virtuelle Infrastrukturen ganzer Unternehmen überwachen und verwalten können.

Das System erlaubt es, die Sicht in unterschiedlichen Ebenen aufzufächern. So können die Administratoren eine Aufteilung von großen Bereichen wie dem Rechenzentrum, ESX-Clustern, Ressourcen-Pools, gemeinsam genutzte Speicherbereiche bis hinunter zu einzelnen virtuellen Maschinen vornehmen. Dabei lassen sich die Ressourcen wie CPU, Memory, Disks oder NICs festlegen und zeitlich erfassen.

Einstiegsgehälter

Im Zuge der Umstellung auf internationale Hochschulabschlüsse Bachelor und Master bleibt das Gehaltsniveau der Studienabsolventen in Deutschland konstant. Durchschnittlich verdient ein Bachelor-Absolvent 39 000 €. Das Gehalt eines Masters liegt um 3000 € höher.

Die vergleichende Analyse aktueller Kienbaum-Vergütungsstudien zeigt, dass der Master analog dem Universitätsabschluss und der Bachelor analog dem Fachhochschulabschluss vergütet wird. Der Untersuchung zufolge schwanden zudem die Vergütungsunterschiede zwischen Universitäts- und Fachhochschulabsolventen in den vergangenen Jahren. Das Einstiegsgehalt eines Ingenieurs mit Fachhochschulabschluss beträgt heute durchschnittlich 41 000 € im Jahr. Für einen Universitätsabschluss erhält man lediglich 2000 € mehr. Vor vier Jahren betrug der Unterschied noch 3000 €.

KURZ NOTIERT

Gefragt: SAP-Experten bleiben die gefragten Spezialisten unter den IT-Freiberuflern. Im letzten Jahr erhielten sie über 32 000 Projektofferten über das Gulp-Portal. Die erhöhte Nachfrage schlug sich in den Stundensatzforderungen nieder. Zu Jahresbeginn forderten externe SAP-Profis einen durchschnittlichen Stundensatz von 81 €. Dieser Wert stieg im Jahresverlauf auf gegenwärtig 84 € pro Stunde.

Mangel: Laut einer Bitkom-Umfrage beabsichtigen 57 % der ITK-Firmen – vornehmlich Softwarehäuser und IT-Dienstleister – im laufenden Jahr zusätzliche Mitarbeiter einzustellen. Nur jedes elfte Unternehmen will Stellen streichen. 65 % der Unternehmen gaben zudem an, dass der Mangel an IT-Experten ihre Geschäfte bremst. Jedes vierte Unternehmen muss Aufträge ablehnen, weil Mitarbeiter fehlen.

Stellenanzeigen: Wissen gegen Erfahrung

Deutsche IT-Unternehmen besetzen offene Stellen für Programmierer bevorzugt mit Hochschulabsolventen. Rund 30 % der Stellenanzeigen betreffen Berufseinsteiger und Nachwuchsentwickler, nur halb so viele (14 %) Jobausschreibungen richten sich an gestandene Anwendungsentwickler, die bereits längere Zeit im Berufsleben stehen. Im Stellenmarkt für IT-Architekten suchen Personalchefs dagegen deutlich öfter erfahrene IT-Profis als Berufseinsteiger. Von den Stellenangeboten für Berufserfahrene richten sich 13 % an Spezialisten im Aufbau von IT-Architekturen. Absolventen werden dagegen in diesem Einsatzgebiet mit unter 5 % erheblich weniger gesucht. Vergleichbares gilt für das Projektmanagement. Auch hier sucht man IT-Experten mit Berufserfahrung (9,8 %) deutlich häufiger als Berufseinsteiger (2,7 %). Zu diesen Ergebnissen gelangt die Studie „IT Jobscout 2008“ der PPI AG.

Verwaltungsvorgänge beschleunigen

Dienstlich

Tobias Haar

Den Traum vom One-Stop-Government soll die EU-Dienstleistungsrichtlinie einen entscheidenden Schritt voranbringen. Ziel sind stark auf IT gestützte durchgängige und medienbruchfreie Verwaltungsprozesse in der EU. Gut vorbereitete IT-Dienstleister dürfen auf volle Auftragsbücher hoffen.

Die EU-Dienstleistungsrichtlinie soll die grenzüberschreitende Erbringung von Dienstleistungen innerhalb der EU und damit den einheitlichen Binnenmarkt fördern. Sie soll die Zulassung zur Dienstleistung in einem anderen EU-Land erleichtern. Die Intention ist, Dienstleister aus anderen Ländern in die Lage zu versetzen, sich über die entsprechenden Zulassungsregelungen aus der Ferne informieren sowie Anträge von dort aus stellen und Bescheide empfangen zu können.

Auf Verwaltungsebene soll es eine verbesserte Zusammenarbeit der europäischen Verwaltungen geben. Schließlich sollen einheitliche Qualitätsstandards und Verhaltenskodizes für Dienstleistungserbringer geschaffen werden.

Die Richtlinie müssen die einzelnen EU-Staaten bis Ende 2009 umsetzen. Sie gilt grundsätzlich für alle „im Wirtschaftsverkehr gehandelten Dienstleistungen“. Ausgenommen sind nur besonders geregelte oder sensible Bereiche, etwa Gesundheitsleistungen, die elektronische Kommunikation, private Sicherheitsdienste, Arbeitsrecht et cetera. Obwohl die Richtlinie bereits von 2006 ist, kommt durch die knappe verbleibende Zeit derzeit deutlich Bewegung in ihre Umsetzung.

Zwang zu E-Government

In der Richtlinie setzt die EU massiv auf die IT-Unterstützung entsprechender Prozesse. Alle Verfahren und Formalitäten sollen mittels IT abgewickelt und die zuständigen Behörden über sie verbunden werden. Dazu gilt es, EU-weit Prozesse und Schnittstellen zu definieren. Gerade die Herausforderung, Verwaltungshandeln an Prozessen und nicht an Aufgaben zu orientieren, muss zu einem erheblichen Mentalitätswandel in der öffentlichen Verwaltung führen. Gleichzeitig müssen Interoperabilität, Datenschutz und Sicherheit gewährleistet sein, um einerseits Medienbrüche zu vermeiden und andererseits die Integrität der Prozesse im Einklang mit sonstigem geltenden Recht zu verwirklichen. Ohne IT-Dienstleister aus der Privatwirtschaft wird die Umsetzung nicht gelingen.

Interessant ist die Richtlinie aus IT-rechtlicher Sicht insbesondere, weil sie zum ersten Mal einen „rechtlichen Zwang zur Realisierung von E-Government-Anwendungen“ festschreibt. In Deutschland werden diese Aspekte der Richtlinie nun unter der Federführung der Länder Baden-Württemberg und Schleswig-Holstein umgesetzt. Das entsprechende Projekt trägt den Namen „Deutschland-Online“. Bis Mitte 2008 sollen Blaupausen für die IT-Umsetzung in den Ländern vorliegen, die die Behörden anschließend erproben. Im Ergebnis soll dies zur Definition der infrastrukturellen Anforderungen in Deutschland im europaweiten Kontext führen.

Daneben gilt es, die IT-Architektur und die medienbruchfreie Verfahrensabwicklung zu entwickeln. Schließlich sollen die Verantwortlichen technische Standards für Schnittstellen vorschlagen sowie die rechtlichen und organisatorischen Anforderungen einer elektronischen Verfahrensabwicklung zeigen. Bei alldem ist darauf zu achten, dass im föderalen Deutschland nicht entlang der Grenzen der Bundesländer Insellösungen entstehen.

Bei der Umsetzung sind gerade die IT-spezifischen Regelungen der Richtlinie von besonderem Interesse. Die lassen sich wiederum in Regelungen des Verhältnisses zwischen Bürgern oder Unternehmen und Staat (Consumer-to-Government, C2G, Business-to-Government, B2G) sowie der EU-Staaten untereinander (Government-to-Government, G2G) unterteilen. Im B2G-Verhältnis geht es um ein elektronisches Antragsverfahren über einen einheitlichen nationalen Ansprechpartner oder die zuständige Behörde.

Daneben sollen Dienstleistungsempfänger – also Kunden – sowie der Dienstleister selbst Informationen zum eigenen wie zum ausländischen Recht bei dem für ihn zuständigen „einheitlichen Ansprechpartner“ erhalten. Gerade das setzt eine intensive Vernetzung aller betroffenen Stellen im In- und Ausland voraus.

Informationen via IT austauschen

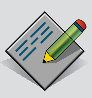
Im G2G-Verhältnis geht es insbesondere um den Aufbau eines „Systems europäischer Amtshilfe“. Behörden müssen EU-weit vernetzt sein, um miteinander kommunizieren zu können. Geplant sind überdies der gegenseitige Registerabruf sowie die Erreichbarkeit von Beschwerdestellen. Hier geht es etwa um die Überprüfung der Angaben ausländischer Dienstleister und um die Überwachung der Tätigkeiten deutscher Dienstleister im Ausland. Dies soll im Wesentlichen das sogenannte „Binnenmarkt-Informationssystem IMI“ ermöglichen.

Die Umsetzung der EU-Dienstleistungsrichtlinie könnte sich zu einem Motor für die IT-Branche in Deutschland und anderen EU-Staaten entwickeln. Laut der Studie Branchenkompass Public Services 2007 von Steria Mummert Consulting planen etwa 30 % aller deutschen Kommunen, den Aufbau, den Betrieb und die Wartung der erforderlichen E-Government-Portale auszuschreiben. 20 % der Behörden erwägen offenbar eine vollständige Auslagerung ihrer IT zu externen Dienstleistern.

Die Umsetzung der EU-Dienstleistungsrichtlinie eröffnet IT-Unternehmen nicht nur die Möglichkeit, ihre Leistungen in anderen EU-Ländern einfacher und effizienter zu vermarkten, sondern gerade auch die IT-Umsetzung auf etwa kommunaler Ebene mitzugestalten und letztlich auch daran mitzuverdienen. Dazu werden in den kommenden Monaten die Weichen gestellt. Die mit der Umsetzung befassten Juristen sehen sich im Bereich des Verwaltungsrechts mit der Aufgabe konfrontiert, teils jahrzehntealte Vorschriften so anzupassen, dass IT-Infrastrukturen sie abbilden können. Aber genau das bezweckt die Richtlinie: Es soll kein Stein auf dem anderen bleiben. (ur)

Bis Mitte dieses Jahres sollen die Projektbeteiligten von „Deutschland-Online“ Pläne für die IT-Umsetzung der europaweiten E-Government-Vorgaben erarbeiten.

KURZ NOTIERT



Frequenzen für Breitbanddienste: Die Bundesnetzagentur hat bundesweit das bisher größte Funkfrequenzspektrum für breitbandige Anwendungen zur Verfügung gestellt. Neuen Anbietern soll damit und durch Technik- sowie Diensteneutralität der Marktzugang ermöglicht werden.

Tastendruck-Abzocke: Das Verwaltungsgericht Köln hat eine Weiterleitung per Tastendruck auf eine kostenpflichtige Mehrwertdienste-Rufnummer für unzulässig erklärt, da dies gleich gegen mehrere Gesetze verstößt. Damit wurde eine Verbotsentscheidung der Bundesnetzagentur gerichtlich bestätigt.

Löschungspflicht für Unterseiten: Hat ein Gericht die Nutzung einer Internet-Domain untersagt, genügt eine Entfernung der Startseite nicht. Es müssen auch alle Unterseiten gelöscht werden, sonst drohen Bußgelder, hat das Landgericht Düsseldorf entschieden.

Sub-loop Unbundling in der Schweiz: Die Schweizer Kommunikationskommission hat der Swisscom aufgegeben, bis Juli 2008 ein Angebot zum Sub-loop Unbundling vorzulegen. Damit soll auch die letzte „halbe Meile“, die Leitung vom Verteilerkasten zum Hausanschluss, für Konkurrenten zugänglich werden.

Internet-Sperrungsverfügungen: Die medienwirksame Anordnung der Sperrung von Internetseiten durch die Düsseldorfer Bezirksregierung im Jahr 2002 war rechtswidrig. Dies hat nun ein Rechtsgutachten ergeben. Diesem zufolge fehlt es für derlei Maßnahmen an gesetzlichen Rechtsgrundlagen.

Impressumspflicht: Die Impressumspflicht nach dem Telemediengesetz gilt auch dann für gewerbliche Internet-Inhalte, wenn diese Webseiten über fremde Server (Host Provider) ins Internet gelangen. Das belegt ein neues Urteil des Oberlandesgerichts Düsseldorf.

Keine Fax-Pflicht für Unternehmer: Das Oberlandesgericht Hamburg hat die lang umstrittene Frage entschieden, ob Unternehmer im Fernabsatz für den Widerruf des Vertrages durch einen Verbraucher ein Telefax vorhalten und die Nummer angeben müssen. Die hanseatischen Richter haben das nun verneint.

Nutzungsverbot betrifft auch Subdomains

Vor einiger Zeit wurde Google die Nutzung des E-Mail-Dienstes unter „gmail.com“ in Deutschland verboten. Ein entsprechendes Urteil erstritt der Inhaber der Webseite „gmail.de“, der auch die zugehörige Wortmarke besitzt. Das Oberlandesgericht Hamburg (Az. 5 W 102/07) verhängte nun ein Bußgeld, weil Google unter einer Subdomain (m.gmail.com) ein Forwarding eingerichtet hatte. Damit wurde der unter gmail.com eingehende E-Mail-Verkehr auf eine andere Domain umgeleitet. Die Verwendung der Subdomain ist nach Auffassung der Richter aber ebenso als Markenverletzung anzusehen. Das Gleiche dürfte auch beim „Redirecting“ gelten.

Tobias Haar

Verbraucherschutz bei gewerblichem Verkauf

Das Widerrufsrecht im Fernabsatz steht nur Verbrauchern, nicht aber gewerblichen Kunden zu. Das Oberlandesgericht Hamm (Urteil vom 28.02.2008, Az.: 4 U 197/07) hat nun entschieden, dass dieser Grundsatz auch dann gilt, wenn ein gewerblicher Anbieter auf Ebay defekte Hardware zum Ausschlachten anbietet, obwohl dessen AGB einen Verkauf „ausschließlich an Gewerbetreibende“ vorsehen. Für die Richter kann der AGB-Hinweis zu leicht übersehen werden, um wirksam zu sein.

Tobias Haar

Usenet-Betreiber haften doch

Bislang haben die meisten deutschen Gerichte eine Haftung von Usenet-Betreibern für Rechtsverletzungen der über sie abrufbaren Inhalte abgelehnt. Nicht so das Landgericht Hamburg in gleich mehreren Entscheidungen. Da Anbieter „recht offensichtlich mit Urheberrechtsverletzungen per AdWords warben“, hatte Google diese aus seinem Werbeprogramm ausgeschlossen. Die dagegen gerichteten Klagen wies das Gericht mit der Begründung ab, der Beklagten Google nicht zumuten zu können, „mit in die Haftung genommen zu werden, wenn sie Werbung von solchen Providern“ ermöglichen muss. Damit haben die Richter erkennen lassen, dass sie auch eine Haftung nur des Werbeanbieters für möglich halten.

Tobias Haar

Haftung für Affiliate-Vertriebspartner

Werden bei einem Internet-Vertriebssystem Produkte über Affiliates vertrieben, haftet der Verkäufer auch für Wettbewerbsverstöße seiner Vertriebspartner. Das gilt selbst dann, wenn sich die Vertriebspartner vertraglich zur Einhaltung der geltenden Gesetze verpflichtet haben. Mit dieser Begründung urteilte das Oberlandesgericht Köln (Az. 6 U 149/07) im Fall einer Affiliate-Webseite, die gegen lebensmittelrechtliche Vorschriften verstoßen hatte. Die Richter waren der Meinung, dass es sich bei Affiliates um „Mitarbeiter“ oder „Beauftragte“ im Sinne des Gesetzes gegen den unlauteren Wettbewerb handelt. Deren Fehlverhalten muss sich der „Merchant“ also zurechnen lassen. Alle Betreiber solcher Vertriebssysteme sollten ihre Partner künftig stärker überwachen. Rein vertragliche Regelungen schützen im Zweifel nicht vor gerichtlicher Inanspruchnahme.

Tobias Haar

Outsourcing berechtigt zur Kündigung

Ein Unternehmer darf Mitarbeitern einer Abteilung kündigen, die der Arbeitgeber im Wege des Outsourcing aufgibt. Das hat das Bundesarbeitsgericht (Az. AZR 1037/06) entschieden. Im konkreten Fall wurde die bislang von Mitarbeitern erbrachten Leistungen an selbstständige Unternehmer vergeben, um Sozialabgaben zu sparen. Gegen die betriebsbedingten Kündigungen klagten die entlassenen Mitarbeiter und unterlagen nun vor dem höchsten deutschen Arbeitsgericht. Allerdings darf es sich bei einer Outsourcing-Entscheidung nicht um eine willkürliche Maßnahme handeln. Zudem muss ein Unternehmen sie tatsächlich umsetzen. Sie darf nicht nur vorgeschoben sein, um Sozialabgaben zu sparen. Ebenso wenig darf das Unternehmen die „Mitarbeiter“ künftig als Selbstständige weiterbeschäftigen, obwohl sie fest in die Betriebsorganisation eingegliedert bleiben.

Tobias Haar

Weitere Reform des Urheberrechts

Der Bundestag hat mit einer weiteren Reform des Urheberrechts den Kampf gegen Produktpiraterie erleichtert und damit das geistige Eigentum gestärkt, so die offizielle Presseerklärung des Bundesjustizministeriums. Werden Verletzungen im „gewerblichen Ausmaß“ vorgetragen, haben künftig etwa auch Accessprovider eine Auskunftspflicht über den Anschlussinhaber, wenn dies ein Richter anordnet. Der „Umweg“ über staatsanwaltschaftliche Ermittlungsverfahren kann in diesen Fällen künftig entfallen. Der Verletzer muss zudem auf Antrag Urkunden vorlegen und Sachen besichtigen lassen, selbst wenn es sich hierbei um Betriebsgeheimnisse handelt. Das Gericht hat aber für angemessenen Schutz der Vertraulichkeit zu sorgen. Auch Verbraucherrechte werden gestärkt, da Abmahngebühren bei Urheberrechtsverletzungen künftig nur noch 100 Euro betragen dürfen.

Tobias Haar

IBM: Ereignisse zu Muster zusammenfügen

Mit Websphere Business Events erweitert IBM sein Portfolio für die Ereignisverarbeitung in serviceorientierten Architekturen. Das Werkzeug beruht auf der Technik des im Januar übernommenen Anbieters Aptsoft und soll Verbindungen zwischen verschiedenen Ereignissen erkennen. Im Idealfall kann die Software automatisch die Muster analysieren und aufgrund von Geschäftsregeln eine Aktion ohne menschliche Hilfe anstoßen. Laut IBM ist das Programm in der Lage, mehr als zehn Millionen Transaktionen täglich zu analysieren. Beispielsweise soll es Muster für betrügerische Tätigkeiten aufdecken, Produktfehler finden oder Verkaufschancen identifizieren. Business Events wendet sich an Geschäftsanwender, das heißt, die Ereignisse sind deklarativ in der entsprechenden Begrifflichkeit beschrieben und sollen sich leicht ändern lassen. Regel-Templates helfen dem Benutzer dabei, Muster oder Filter für bestimmte Aktionen zu erstellen. *Susanne Franke*

SAP: Komplettangebote für den Mittelstand

Sowohl mit HP als auch mit IBM will SAP vorinstallierte Business-All-in-one-Lösungen vermarkten. Die HP-Variante soll auf Proliant-Maschinen oder Servern aus der Reihe Bladesystem c3000 laufen. Zielgruppe sind mittelständische Unternehmen aus den Bereichen Fertigung, Dienstleistungen und Handel. Das Angebot basiert auf dem kürzlich vorgestellten Fast-Start-Programm für Business All-in-one. Neben der ERP-Software umfasst das Paket die Datenbank MaxDB sowie das Betriebssystem Suse Linux Enterprise Server von Novell.

Auch die Partnerschaft mit IBM wird intensiviert. Die beiden Firmen planen, ihre Angebote für den Mittelstand zu kombinieren. Diese Offerte läuft wahlweise auf IBM System x, Bladecenter oder Power Systems. Zudem beinhaltet sie Datenbank (MaxDB oder DB2) und Betriebssystem (Suse Linux Enterprise Server). Beide Pakete kommen laut SAP noch dieses Jahr auf den Markt.

Kooperation für sicheres Banking

ACI Worldwide und Eunexus bieten eine gemeinsame Lösung zum Eindämmen von Betrug und Missbrauch beim Internet-Banking an. Eunexus integriert seine IP-Profiling-Technik, die verdächtige IP-Adressen erkennt, in ACIs Proactive Risk Manager. Dieses Programm überwacht Transaktionen in Echtzeit und alarmiert das Finanzinstitut oder stoppt den Buchungsvorgang, wenn er von einer verdächtigen IP-Adresse ausgelöst wird. Eunexus verkauft Security- und Fraud-Produkte für Internet-Anwendungen, ACI Lösungen für den elektronischen Zahlungsverkehr.

Crossgate offeriert EDI-Flatrate

Für eine fixe monatliche Gebühr will Crossgate einen schnellen und stressfreien Einstieg in die EDI-Welt anbieten. Das Komplettpaket enthält eine lebenslange Garantie, die jede künftige Anforderung abdeckt, egal ob es sich um den Ausbau, neue Kundenwünsche oder das Zollverfahren ATLAS handelt. Die in drei Stufen verfügbare monatliche Flatrate deckt Softwarewartung, Support, ein Freivolumen an Geschäftspartnerprofilen sowie ATLAS ab. Dem Kunden der insolventen Mosaic Software AG macht Crossgate ein Migrationsangebot (www.crossgate.de).

KURZ NOTIERT

Einkauf: EMC schloss mit der Iomega Corporation eine Akquisitionsvereinbarung. Demzufolge wird man den Plattenspeicherspezialisten für etwa 213 Mio. $ übernehmen. Iomega soll zentraler Bestandteil des neuen Geschäftsbereichs „Consumer/Small Business Products Division“ bei EMC werden.

Gesichert: IBM erwarb Diligent Technologies, einen Spezialisten auf dem Feld der sogenannten Deduplikationstechnologie. Die Übernahme ist die dritte speicherbezogene Akquisition der IBM in jüngster Zeit. Im Januar hat Big Blue XIV gekauft, Anfang April traf IBMs Interesse FilesX.

Einstieg: Perot Systems Corporation übernimmt die „HighQ IT for the manufacturing industry“ (HighQ IT) aus Ottobrunn. Durch den Kauf will der US-amerikanische IT-Dienstleister sein Angebot an SAP-Services und industriespezifischen Beratungen vergrößern. Das Unternehmen „HighQ IT for the financial industry“ ist nicht Bestandteil der Übernahme.

Lichtblick: Nokia geht, RIM (Research in Motion) kommt. Der Backberry-Hersteller beabsichtigt, in Bochum ein Forschungszentrum aufzubauen. Noch in diesem Sommer sollen dort 140 bis 180 Mitarbeiter eine Beschäftigung finden und Hard- und Software für Smartphones entwickeln. Für das erste Jahr plant RIM Investitionen in Höhe von 45 Mio. $.

Mit Power: Infineon Technologies verstärkt seine Aktivität im Bereich der Energie-Management-Applikationen mit der Übernahme von Primarion. Das Unternehmen zählt zu den Spezialisten in den Bereichen Design, Fertigung und Marketing von Chips für digitales Power-Management in Computer-, Grafik- und Kommunikationssoftware.

Hightech-Branche in Europa

Wachstum verlangsamt

Achim Born

Der ITK-Markt legt laut dem European Information Technology Observatory (EITO) in ganz Europa weiter zu. Unter den großen Ländern sind Spanien und Frankreich die boomenden Märkte.

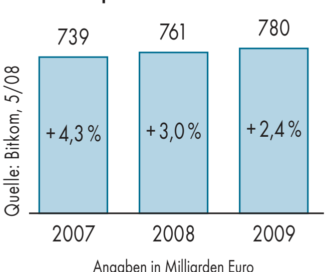
Der europäische Markt für IT, Telekommunikation und digitale Unterhaltungselektronik wird dieses Jahr voraussichtlich um 3 % auf 761 Mrd. € wachsen. Dies vermeldet der Bitkom mit Blick auf die jüngste EITO-Statistik. Im kommenden Jahr soll sich das Wachstum auf etwas niedrigerem Niveau (2,4 %) auf dann 780 Mrd. € fortsetzen. Unter den großen Ländern wachsen heuer Spanien mit 4,6 % und Frankreich mit 3,2 % am stärksten. Neuer Umsatz-Spitzenreiter ist jedoch Großbritannien. Mit einem Marktvolumen von 152 Mrd. € liegt das Vereinigte Königreich vor Deutschland, das 145 Mrd € aufweist. Als Grund führen die Bitkom-Vertreter das Outsourcing-Geschäft an, da britische Unternehmen und Behörden in der EU mit Abstand am stärksten ihre IT auslagern. Hierzulande würden vergleichbare Leistungen oft noch firmenintern erbracht und flössen daher nicht in die Marktstatistik ein.

Die stärksten Impulse liefert die Informationstechnik. Der IT-Markt legt derzeit EU-weit um 4,3 % auf 313 Mrd. € zu. Wenig überraschend boomen innerhalb dieses Segments vor allem IT-Services (5,7 %) und Software (5,2 %). Bei IT-Services verzeichnet der Outsourcing-Markt mit 7,4 % das höchste Plus. Für das kommende Jahr rechnet man beim EITO europaweit mit einem Plus von 4,4 % auf 326 Mrd. €.

Im Telekommunikationssektor fällt das Wachstum dieses Jahr nicht nur in Deutschland vergleichsweise gering aus. Europaweit wächst der TK-Markt 2008 um 2 % auf 386 Mrd. €. Während die Umsätze mit Festnetzgesprächen rückläufig sind, gibt es starke Zuwächse bei Datendiensten. Mit rund 11 % Umsatzplus boomen sowohl feste Internet-Zugänge und Dienste als auch mobile Datendienste. Für 2009 wird auf Europaebene ein Plus von 1,8 % auf 393 Mrd. € im Telekommunikationsmarkt erwartet.

Die Nachfrage nach digitaler Unterhaltungselektronik steigt ebenfalls. Die Umsätze wachsen 2008 um 2,5 % auf 63 Mrd. €. Dominant sind hier die Geschäfte mit flachen TV-Geräten, die 40 % des Marktvolumens ausmachen. Es folgen Digitalkameras mit 11 % und Spielkonsolen mit 8 %. Da inzwischen viele Haushalte diese digitalen Geräte besitzen und gleichzeitig die Preise fallen, sollen im Jahr 2009 die Umsätze auf dem europäischen CE-Markt um 3,2 % auf 61 Mrd. € zurückgehen. (WM)

Europäischer ITK-Markt



Angaben in Milliarden Euro

Fujitsu Siemens schrumpft – Partnerschaftsvertrag erstmals kündbar

Das im vergangenen Jahr formulierte Umsatzziel erwies sich für FSC (Fujitsu Siemens Computers) als zu hoch. Statt die 7-Mrd.-€-Marke beim Umsatz zu passieren, musste man einen Rückgang von 4,9 % auf 6,6 Mrd. € für das Geschäftsjahr 2007 melden. Immerhin konnte das Unternehmen im Zeitraum April 2007 bis März 2008 den Vorsteuergewinn um 15 % von 91 Mio. auf 105 Mio. € steigern. Die ursprünglich angestrebte Vorsteuer-Rendite von 2 % konnte FSC damit zwar nicht erreichen. Die aktuellen 1,6 % erachtet das Management im Vergleich aber als „gar nicht so schlecht“.

Ungeachtet der Marktschwierigkeiten ist FSC-Chef Bernd Bischoff optimistisch, dass die Investitionen in den Auftritt als Infrastrukturanbieter und des Service-Portfolios sich in Bälde auszahlen. Spannend werden die kommenden Monate für FSC allemal, denn im neuen Geschäftsjahr besteht für Fujitsu oder Siemens die Möglichkeit, den auf zehn Jahre geschlossenen Partnerschaftsvertrag erstmalig zu beenden.

Suchen im eigenen Datenbestand

Das Interesse an unternehmensinternen Suchmaschinen steigt in Deutschland stetig, meldet die Experton Group. Für das laufende Jahr erwartet die Marktforschungsfirma, dass die Unternehmen für entsprechende Projekte 61,4 Mio. € ausgeben. 2009 sollen es schon 18 % mehr sein. Das Marktvolumen für 2010 wird auf knapp 85 Mio. € veranschlagt. Neben eigenen internen Anforderungen sollen zusätzlich externe Faktoren wie die Einhaltung von Compliance-Anforderungen den Einsatz professioneller Suchlösungen in Unternehmen vorantreiben.

Freenet kauft Debitel und übernimmt Schulden

United-Internet-Chef Ralph Dommermuth mühte sich vergebens. Eckhard Spoerr, Vorstandsvorsitzender der Freenet AG, ließ sich weder durch gutes Zureden noch Drohungen vom Kauf der Debitel Group abbringen. Die Übernahme umfasst im Wesentlichen die Debitel AG, die Talkline GmbH und die _dug telecom ag. Offizielle Verkäuferin ist die von den Permira Fonds mehrheitlich kontrollierte Holding „Debitel (Netherlands) Holding BV“. Diese erhält als Gegenleistung von freenet 32 Mio. neue Aktien, was 24,99 % und einem Wert von rund 360 Mio. € entspricht, sowie ein langfristiges verzinsliches Verkäuferdarlehen von 132,5 Mio. €. Zugleich übernimmt Freenet die über einer Milliarde Euro Schulden der Debitel Group, sodass sich der Kaufpreis auf insgesamt 1,63 Mrd. € summiert. Durch die Übernahme von Debitel sieht sich die Freenet AG als führendes netzunabhängiges Telekommunikations- und Internet-Unternehmen in Deutschland. Bis zum Vollzug des Kaufs wird allerdings noch ein wenig Zeit verstreichen, da man noch die börsentechnischen Voraussetzungen für die Ausgabe neuer Aktien schaffen muss. Die Zustimmung des Bundeskartellamtes steht ebenfalls aus.

Gewinn der SAP bricht ein

Nach einhelliger Ansicht von Finanzexperten hat SAP das Auftaktquartal kräftig vermasselt. Zwar steigerte das Walldorfer Softwarehaus die Einnahmen mit Softwarelizenzen und -wartung im zweistelligen Prozentbereich: Den Analysten war das jedoch zu wenig. Sie hatten für Software und softwarebezogene Serviceerlöse mit 1,83 Mrd. € gerechnet.

Ähnliches gilt für das Konzernergebnis. Hier hatte man aufgrund der Business-Objects-Übernahme zwar einen Rückgang auf 290 Mio. € eingeplant, mit 242 Mio. € verfehlte SAP diesen Wert jedoch überdeutlich. Allerdings muss man SAP zugutehalten, dass ohne Wechselkurseinfluss das Betriebsergebnis wesentlich erfreulicher ausgefallen wäre.

Neben dem mageren Ergebnis ruft die Verzögerung des neuen Mittelstandsproduktes Business ByDesign Stirnrunzeln bei den Finanzanalysten hervor. Die Vermarktungspläne der von SAP im Mietmodell (Software as a Service) offerierten Lösung wurden einer deutlichen Revision unterzogen. So soll sich die Markteinführung 2008 auf die sechs Länder konzentrieren, in denen die aktuellen Kunden ansässig sind; erst 2009 werden mehr Länder folgen. Des Weiteren erwartet SAP, dass es rund 12 bis 18 Monate länger dauern wird, das ursprünglich für 2010 anvisierte Ziel von 1 Mrd. $ Umsatz und 10 000 Kunden zu erreichen. Im laufenden Jahr geht man nun auch von deutlich weniger als 1000 Kundenprojekten aus.

Infolge der angepassten Pläne reduziert SAP die Investitionen in die neue Software 2008 um rund 100 Mio. €, was auf der anderen Seite zwangsläufig einen positiven Effekt auf die operative Marge ausübt. Ab 2009 soll es auch keine zusätzlichen Investitionen mehr geben. Stattdessen sollen die Kosten in Bezug auf Business ByDesign aus dem operativen Geschäft finanziert werden.

SAP-Bilanz für Q1 2008

	Q1 2008	Q1 2007	Veränderung	ohne Währungseffekt
Softwareerlöse	622	562	11	18
Service	1736	1515	15	24
Umsatz	2460	2162	14	22
Betriebsergebnis	359	436	-18	20
Konzernergebnis	242	310	-22	–

Alle Daten vorläufig
Umsatzzahlen in Millionen Euro
Veränderungen in Prozent

Quelle: SAP 4/2008

Optimistische ITK-Branche

Die ITK-Industrie Deutschlands blickt weiterhin mit Zuversicht auf die Geschäftsentwicklung dieses Jahres. 73 % der Unternehmen erwarten steigende Umsätze. 17 % rechnen mit einem stabilen Geschäft und nur 10 % mit Rückgängen. Das geht aus der aktuellen Umfrage des ITK-Lobbyverbandes Bitkom hervor. Wie in den früheren Umfragen prognostizieren insbesondere die Softwarehäuser und IT-Dienstleister gute Geschäfte. 79 % der in diesem Segment tätigen Anbieter erwarten 2008 steigende Umsätze. Fast drei Viertel gehen zudem von höheren Gewinnen aus. Auch zwei Drittel der Hersteller von Computern und anderen IT-Geräten erwarten ein Umsatzplus.

Micro Focus will Netmanage

Den Aktionären von Netmanage hat Micro Focus einen Aufschlag von rund 73 % gegenüber dem Schlusskurs vom 30. April 2008 angeboten. Der Gesamtwert liegt somit bei 73,3 Mio. $, wobei das Barvermögen von Netmanage mit rund 25 Mio. $ eingeschlossen ist. Die Zustimmung der Anteilseigner von Netmanage soll bis Juni 2008 vorliegen.

Initiative gegen Fachkräftemangel

Zum 5. Mai fiel der Startschuss der Initiative „MINT – Zukunft schaffen“. Ziel der Wirtschaftsverbände BDA und BDI ist es, vermehrt Fachkräfte mit den Qualifikationen in den Fächern Mathematik, Informatik, Naturwissenschaften und Technik (MINT) zu gewinnen. Schüler und Schülerinnen ab der 8. Klasse und deren Lehrkräfte will man gezielt ansprechen, um die Zahl der Studienanfänger sowie Ausbildungsbewerber in den einschlägigen Disziplinen zu erhöhen. In den kommenden sechs Jahren will die Initiative den Projekten der Verbände und Unternehmen mit dem Portal www.mitzukunft.de eine Multiplikationsplattform bieten.

Yang ziert sich, Ballmer will nicht mehr

Die Bestrafung folgte auf dem Fuß. Das Scheitern der Fusionsgespräche zwischen Microsoft und Yahoo führte bei Börseneröffnung am Montag, den 5. Mai, zu einem Kurseinbruch von rund 20 % bei den Papieren des Internet-Portalbetreibers. Die Aktie von Microsoft legte dagegen um 4,5 % zu. Am Samstag zuvor hatte Microsoft-Chef Steve Ballmer überraschend den Schlussstrich gezogen. „Trotz unserer Bemühungen, die auch eine Erhöhung des Gebots um rund 5 Mrd. $ umfasste, hat Yahoo unser Gebot nicht angenommen“, heißt es in dem veröffentlichten Schreiben. Insgesamt hatte Ballmer rund 50 Mrd. $ geboten. Die 33 $ je Aktie – 2 $ mehr als zu Beginn des Kaufangebots – waren dem Yahoo-Gründer und Chef Jerry Yang noch immer zu wenig. Er forderte zum Schluss mindestens 37 $ – wenn nicht gar 38 $ – pro Papier. Nicht wenige Beobachter waren davon überzeugt, dass Yang überhaupt nicht verkaufen wollte.

Allgemein hatte man entweder mit einer Einigung auf Basis von 34 $ oder mit dem Versuch einer feindlichen Übernahme gerechnet. Schließlich hätte das Schlussangebot für Inhaber von Yahoo-Papieren ein Plus von mehr als 70 % gegenüber dem Kurs vor der Offerte Ende Januar bedeutet. Entsprechend harsch fielen die ersten Kommentare von Börsenanalysten und Vermögensverwalter aus. Falls es Yang in absehbarer Zeit nicht gelingt, einen weißen Ritter aus dem Hut zu zaubern, wird eine Klageflut seitens der Aktionäre nicht lange auf sich warten lassen.

Siemens-Gewinn schwindet

Einen Gewinneinbruch meldet Siemens für das zweite Geschäftsquartal (Januar bis März). Den Umsatz konnte der Münchener Konzern, dessen Schmiergeldaffäre die Schlagzeilen der Wirtschaftsgazetten dominiert, zwar um 1 % auf 18 Mrd. € ausbauen. Der Gewinn nach Steuern betrug dagegen nur noch 412 Mio. €, nach 1,2 Mrd. € in der Vorjahresperiode. Die Rückgänge sind hauptsächlich auf das Ergebnis des operativen Geschäftes zurückzuführen. In der Kraftwerkssparte fehlten in erster Linie Ingenieure zum Bewältigen von Aufträge. Die Transportsparte litt weiterhin unter der störanfälligen Niederflur-Straßenbahn Combino. Schlecht liefen auch die Geschäfte des Bereichs IT Solutions and Services mit einem Umsatz von 1,3 Mrd. € (-6 %).

Für den weiteren Geschäftsjahresverlauf gibt sich der neue Siemens-Chef Peter Löscher „verhalten optimistisch“. Der Umsatz soll im Gesamtjahr um rund 6 % zulegen. Das operative Ergebnis soll – trotz des Einbruchs im zweiten Quartal – das Vorjahresniveau erreichen. Allerdings gibt es weiterhin einige Unbekannte in der Siemens-Bilanz. Es steht noch der Verkauf der darbenden TK-Anlagensparte SEN aus, der einige Belastungen nach sich ziehen wird. Des Weiteren bereitet die Korruptionsaffäre noch enorme Kosten. Allein die hier tätigen Ermittler und Berater sollen Siemens im zweiten Quartal 175 Mio. € gekostet haben, von zu erwartenden steuerlichen Nachforderungen und Strafzahlungen ganz zu schweigen.

Mieses Quartal für Sun

Die schwarzen Zahlen sind bei Sun erst einmal wieder vorbei. Zumindest gilt dies für das im März beendete dritte Geschäftsjahresquartal. Weniger Einnahmen als erhofft führten zu einem Nettoverlust von 34 Mio. $. Der Umsatz fiel im Vergleich zum Vorjahr mit 3,3 Mrd. $ etwas niedriger aus. Als Erklärung nannte das Sun-Management den Kauf von MySQL und die schwächelnde US-Konjunktur. Für Sun ist die Entwicklung alles andere als erfreulich. Bis zu 2500 der rund 34 400 Mitarbeiter müssen nun befürchten, ihre Arbeit zu verlieren.



Arbeitspferde für kleinere Unternehmen

Linux en miniature

Christian Böttger

Kleinere Unternehmen interessieren sich nicht wirklich für die Technik eines Servers – er soll einfach ihren Bedarf abdecken und laufen. Dies lässt sich nicht nur mit Microsofts Small Business Server, sondern immer besser auch mit Linux-basierten Systemen erreichen.

Vor allem kleinere Firmen haben besondere Anforderungen: Sie haben kein Geld zum Aufbau einer umfangreichen Infrastruktur, daher sollten alle Funktionen auf einem einzigen Server vorhanden sein – unter Beachtung eines ausreichenden Sicherheitsniveaus. Letzteres behandelt der Artikel „Lochmuster“ in dieser Ausgabe [1]. Auch existiert oft weder umfangreiches IT-Wissen noch genügend Zeit zur Betreuung komplexer Systeme. Die müssen also einfach einzurichten und zu handhaben sein. Deshalb ist eine einheitliche grafische Oberfläche für alle Funktionen unverzichtbar. Kommandozeilen-Tools können höchstens als Ergänzung zum Einsatz kommen.

Den Takt gibt in diesem Markt – wieder einmal – Microsoft mit dem Small Business Server (SBS) vor. Er arbeitet als Mailserver und stellt Kalender und Adressdaten mit Exchange bereit, bietet Datei- und Druckdienste, eine Verwaltung der Arbeitsplatzrechner mit Push-Updates, eine zentrale Benutzerverwaltung und in der Professional-Version auch einen Datenbankserver (MS SQL). Und alles lässt sich über eine grafische Oberfläche (Serververwaltungskonsole) einheitlich verwalten. Alle Komponenten arbeiten, da sie aus einer Hand stammen, mehr oder weniger reibungslos zusammen. Lediglich der SQL-Server entwickelt ein leichtes Eigenleben.

Natürlich lassen sich die Basisfunktionen eines Servers für kleinere und mittlere Unternehmen (KMU) auch mit Linux-basierten Systemen darstellen. Allerdings sind die großen Distributionen wie Suse Linux Enterprise Server (SLES) oder Red Hats Enterprise Linux (RHEL) eher als eierlegende Wollmilchsäue für größere Firmen zugeschnitten. Um sie in KMU einzusetzen, ist ein nicht unerheblicher Aufwand für das „Zurechtstutzen“ und Konfigurieren einzuplanen. Außerdem fehlt ihnen eine einheitliche Administrationssoftware, mit der sich alle Komponenten aus einem Guss verwalten lassen.

Kandidaten jenseits des Platzhirsches

Debian lässt sich natürlich ebenso einsetzen, zielt aber nicht explizit in diese Richtung, auch Ubuntu kümmert sich derzeit noch eher rudimentär um KMU. Während Novell mit seinem Open Workgroup Server – Small Business Edition eine für kleine Unternehmen angepasste Version bietet, findet sich vergleichbares bei Red Hat derzeit nicht.

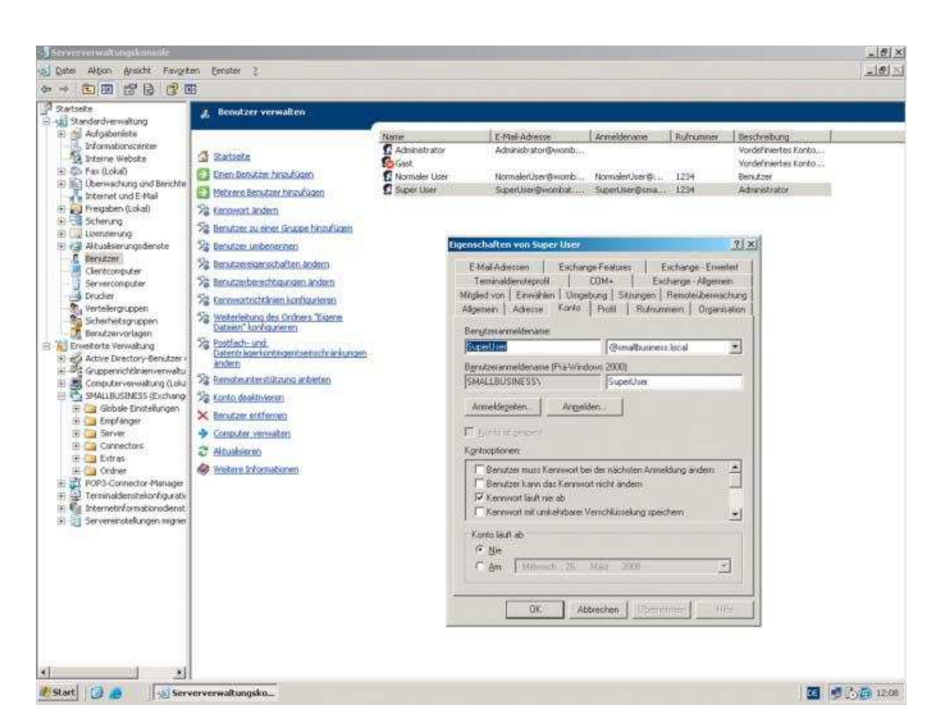
Jedoch auch unabhängig von den „großen“ Distributionen gibt es interessante Ansätze, die sich um einige Linux-Groupware-Lösungen herum herauskristallisiert haben. Mehrere „Linux-SBS“ (Small Business Server) setzen auf das freie Kolab-Projekt als Groupware-Komponente, aber zunehmend gewinnt die proprietäre Lösung Zarafa an Verbreitung. Scalix ist ebenfalls vertreten, zielt aber strukturell eher auf größere Installationen.

Vorreiter auf diesem Gebiet ist Univention mit seinem Corporate Server UCS, der als Groupware-Komponente Kolab einsetzt. Für Freunde anderer Lösungen bieten die Bremer jedoch auch Zarafa oder Scalix als Modul an. Mit dem UCS lassen sich angeschlossene Arbeitsplätze verwalten.

Collax richtet sich gezielt an kleine Unternehmen, als Groupware ist (gegen Aufpreis) Open-Xchange an Bord. Bei Bedarf liefert man die Lösung als vorkonfigurierte Appliance inklusive Hardware. Collax versucht verstärkt, auch „klassische“ Anbieter von Anwendungssoftware aus der Windows-Welt für eine Portierung auf den Collax Business Server zu gewinnen; hier sind Pentaprise und Sage zu nennen.

Die Linux Information Systems AG (LIS AG) aus München und Berlin bietet mit CoreBiz ebenfalls einen speziell für KMU geeigneten Server, der sich als Baukasten an die Anforderungen anpassen lässt. Als Groupware nutzt die LIS AG ebenfalls das freie Kolab. Die Linux-Spezialisten liefern ihren Server nicht von der Stange, sondern fertig mit den jeweiligen kundenspezifischen Einstellungen – die Betreuung ist sozusagen Pflicht. Linux-Arbeitsplätze lassen sich ebenfalls zentral verwalten.

Aus Kanada stammt der Xandros Server, der nach dem Kauf der Firma Scalix durch Xandros natürlich auf den gleichnamigen Mail- und Groupware-Server setzt. Für den deutschen KMU-Markt eher hinderlich ist, dass große Teile der Administrationssoftware nur auf Englisch existieren.



Microsofts Small Business Server verfügt mit der Managemantkonsole über ein leistungsfähiges Administrationswerkzeug (Abb. 1).

Alle Linux-Varianten setzen auf eine eigene Oberfläche zur Administration, sodass der Nutzer (Administrator) kaum noch mit dem darunter liegenden Linux in Berührung kommt – gut für den Umstieg. Die Oberflächen sind oft, aber nicht immer, webbasiert (Collax, Univention, Novell), einige Hersteller bevorzugen jedoch eine „klassische“ GUI-Anwendung (Microsoft, CoreBiz, Xandros). Den Bedienkomfort eines Microsoft SBS bieten solche Lösungen allerdings leider noch nicht ganz.



Microsoft Small Business Server

Zum Test lag Microsofts SBS in der „Premium Edition Release 2 SP1“ vor. Die Installation erfolgte wie bei allen Systemen in einer virtuellen Maschine unter VMware Server 1.0.4. Als Hostsystem diente ein Linux-x86_64-System unter Opensuse 10.3.

Der SBS umfasst acht CDs: Fünf enthalten den Server, zwei weitere die zusätzliche Software der Premium Edition und die letzte die Updates der Release 2. Bei der Installation erkennt das System die vorhandene Netzumgebung und kann sich beispielsweise eines vorhandenen DHCP-Servers bedienen. Wahlweise lassen sich eigene DHCP- und DNS-Server einspielen. Nach dem Aufspielen des Servers (sprich nach den ersten fünf CDs) startet ein Assistent und fragt alle nötigen Einstellungen ab. Die erfragten Fakten sind sehr umfassend, sodass anschließend kaum Handarbeit nötig ist. Das aktuelle SP2 kann man entweder aus dem Internet herunterladen oder von CD 6 installieren. In jedem Fall sind danach weitere Online-Updates erforderlich; nach dem nächsten Neustart lädt das System nochmals zwischen 50 und 60 Pakete herunter und installiert diese. Ebenfalls auf CD 6 befinden sich die Windows-Updates, die Service Management Console sowie .Net 2.0.

Derzeit basiert der SBS noch auf dem schon etwas in die Jahre gekommenen Windows 2003 Server. Der Zusatz „Small Business“ ist durchaus ernst zu nehmen: Mehr als 75 Client-Lizenzen sind nicht vorgesehen, ebenso wenig wie weitere Windows-Server im Netz. Die Premium Edition umfasst zusätzlich zum normalen SBS einen MS-SQL-Server, den ISA-Server, Frontpage sowie das Business Intelligence Development Studio. Die einzige Hürde im Test stellte der SQL-Server auf CD 7 dar: Er ließ sich erst nach dem Einspielen der Client Tools von CD 8 installieren.

Anschließend präsentiert sich der SBS im gewohnten Windows-Look. Die Administration erfolgt über die grafische Management Console. Hier sind in

iX-TRACT

- Server-Lösungen für kleine und mittlere Unternehmen müssen vor allem funktional vollständig und leicht zu bedienen sein.
- Trotz allen Bedienkomforts für die Administration darf das Sicherheitsniveau der Produkte nicht unberücksichtigt bleiben.
- Es existiert eine Reihe von Linux-Ansätzen, die dem Platzhirsch im KMU-Segment das Revier streitig machen wollen.

Baumstruktur alle Elemente von der Nutzerverwaltung über ADS/Domänen-Administration bis hin zum eingebauten Exchange- und SQL-Server vereint. Wegen der vielen Funktionen dauert es zwar eine Weile, bis der Neuling die gesuchten Dinge findet, aber die Struktur ist insgesamt logisch und alle Parameter sind konfigurierbar – wenn auch manchmal tief in Untermenüs versteckt. Man erreicht die einzelnen Administrationsaufgaben aber auch über den üblichen Weg „Start -> Verwaltung“.

Zum Verbinden eines Arbeitsplatzrechners mit dem SBS muss der Administrator auf dem jeweiligen Client lediglich im Internet Explorer einen bestimmten URL aufrufen; die Client-Konfiguration erfolgt via ActiveX gemäß der im Server eingestellten Vorgaben. Das Basis-Windows muss auf dem Client aber schon vorhanden sein – eine komplette Installation wie bei CoreBiz oder UCS via PXE sieht Microsoft nicht vor. Der Server kann angeschlossene Clients im Betrieb automatisch mit Windows-Updates versorgen. Die Updates kann ein Client direkt aus dem Internet beziehen; bei größeren Umgebungen kann das der Server übernehmen und sie lokal vorhalten.

Natürlich enthält der SBS einen Faxdienst, stellt Drucker bereit und ermöglicht die Zusammenarbeit. Für Letzteres gibt es nicht nur die öffentlichen Ordner im Exchange-Server, sondern auch die Webdienste des eingebauten Sharepoint-Servers. Mit dem ISA-Server liefert der SBS eine Firewall und eine VPN-Verwaltung mit – vom Standpunkt der IT-Sicherheit empfiehlt es sich aber nicht, – unabhängig vom Betriebssystem – den internen Firmenserver gleichzeitig als Internet-Gateway und Firewall einzusetzen.

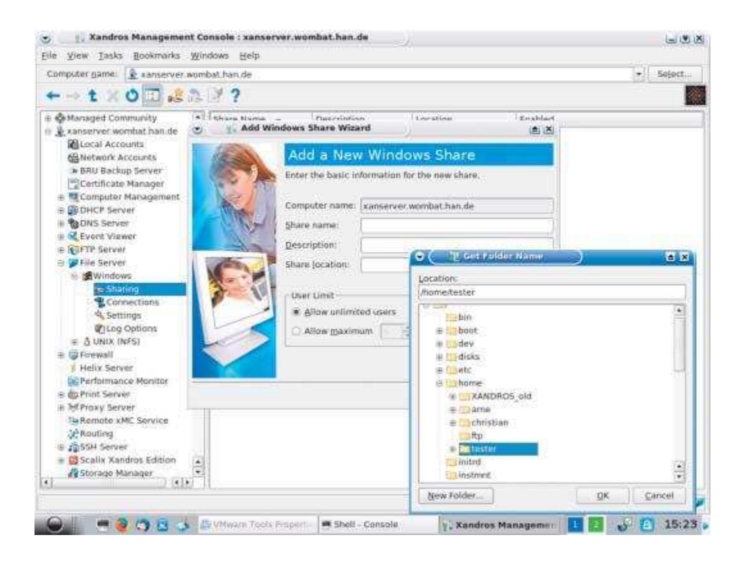
Microsofts SBS lässt sich recht mitteilsam einstellen: Auf Wunsch schickt er dem Administrator per E-Mail Statusmeldungen der einzelnen Dienste. Auch erzwingt er bei jedem Herunterfahren die Eingabe eines Grundes (bei einem Absturz erfolgt die Abfrage beim nächsten Neustart) – für die Qualitätssicherung des Betriebs eine gute Idee.

Wie zu erwarten hinterlässt der SBS insgesamt einen sehr runden Eindruck. Alles ist so, wie man es von Windows erwartet: miteinander integriert, automatisch, nicht immer durchschaubar und mit dem Microsoft-typischen Look & Feel. Ob man das mag oder nicht, muss jeder selbst entscheiden.

Xandros Server

Xandros bewirbt seinen Server als Linux-Lösung für Windows-Umgebungen. Die Zielgruppe sind ganz klar Unternehmen, die zwar die Lizenzkosten für einen Windows-Server sparen, auf den Arbeitsplätzen jedoch weiterhin Windows einsetzen wollen.

Zum Test diente der per Download bezogene Xandros Server in der Version 2. Ihn gibt es als 32- und 64-Bit-Version. Da es allerdings die Groupware Scalix nur in der 32-Bit-Version gibt, ist die 64-Bit-Version des Grundsystems nur sinnvoll, wenn man keine Maillösung braucht. Die Basis ist ein Debian GNU/Linux mit Kernel 2.6.18. Für den deutschen Markt gibt es einen gravierenden Nachteil: Weder der Xandros Server noch Scalix sind durchgehend auf deutsch lokalisiert. Xandros’ Eigenentwicklungen etwa liegen nur auf Englisch vor. Stellt man den Server auf Deutsch ein, erhält man einen schwer verdaulichen Sprachenmix serviert.



Xandros lehnt sich mit seinem Verwaltungs-Tool nicht nur optisch an die Redmonder Vorlage an (Abb. 2).

Xandros sieht den Server als Alternative zum Windows Server 2003. Die Administration erfolgt über die GUI-Anwendung namens xMC (Xandros Management Console), über die sich mehrere Rechner in einer „Managed Community“ verwalten lassen. xMC gibt es für Linux und Windows. Sofern man den Server ohne X11 installiert, muss man die xMC auf einem anderen Rechner einspielen. Die Installationsroutine fragt die nötigen Parameter ab, auch eine Integration mit vorhandenen DHCP- und DNS-Servern klappte problemlos.

Dass Xandros eine Dual-Boot-Installation mit einem vorhandenen Betriebssystem unterstützt, ist löblich – bei einem Server allerdings überflüssig. Vermutlich handelt es sich um ein Überbleibsel des hauseigenen Linux-Desktops. Die Unterstützung für eine Xen-basierte Installation dagegen kann sich als sehr nützlich erweisen. Nach dem ersten Reboot startet ein „First Start Wizard“, der alle noch nötigen Einstellungen erfragt. Der Server integriert sich gut in ein vorhandenes Netz, beachtet sowohl DHCP als auch DNS, erkennt alle CUPS-Server sowie deren Drucker und bindet sie ein. Insgesamt hat sich Xandros große Mühe gegeben, die Installation so zu gestalten, dass ein Linux-unerfahrener Windows-Admin sie problemlos durchführen kann.

Der Installationsumfang besteht aus einer DVD, die Premium Edition besteht aus zwei zusätzlichen CDs mit weiterer Software: MySQL Community Server, Oracle 10h Express Edition, Acrobat Reader, IBM Websphere Community Edition, JBoss, NoMachine Server, Scalix Server und Clients sowie SugarCRM. Somit ist für so ziemlich jeden Zweck eine Anwendung vorhanden. Grundsätzlich ist die Administration der Zusatzsoftware in die xMC beziehungsweise den „Network Manager“ (Installation und Updates) integriert, für einige Details muss man aber doch die von der jeweiligen Software mitgelieferten Tools bemühen.

Nicht ganz gelungen ist die Integration der Oracle Installation. Benutzt man die Minimalforderungen des Xandros-Servers (40 GByte HD und 512 MByte RAM), dann richtet der Xandros-Installer 775 MByte Swap ein – zu wenig für Oracle, man muss dem System manuell mit *mkswap*, *swapon* & Co. zu Leibe rücken. Zum Abschluss muss der Administrator noch ein Oracle-spezifisches Installationsskript aufrufen – diese Tatsache bekommt er immerhin mitgeteilt.

Leider reagiert der Xandros Server recht sensibel auf abrupte Unterbrechungen. Nach einem Absturz während der Installation musste der Tester manuell per *dpkg --configure -a* aufräumen; immerhin erschien eine entsprechende Meldung. Nach einem weiteren Absturz im Testbetrieb versagte die xMC komplett den Dienst. Das System war so durcheinandergeraten, dass nur noch ein Remote Login durch den Xandros Support weiterhalf. Erst nach mehreren Tagen lief das System wieder. Für den *iX*-Test erfolgte der Support direkt vom Hersteller aus Ottawa auf Englisch – für zahlende deutsche Kunden steht jedoch auch ein deutschsprachiger Support zur Verfügung.

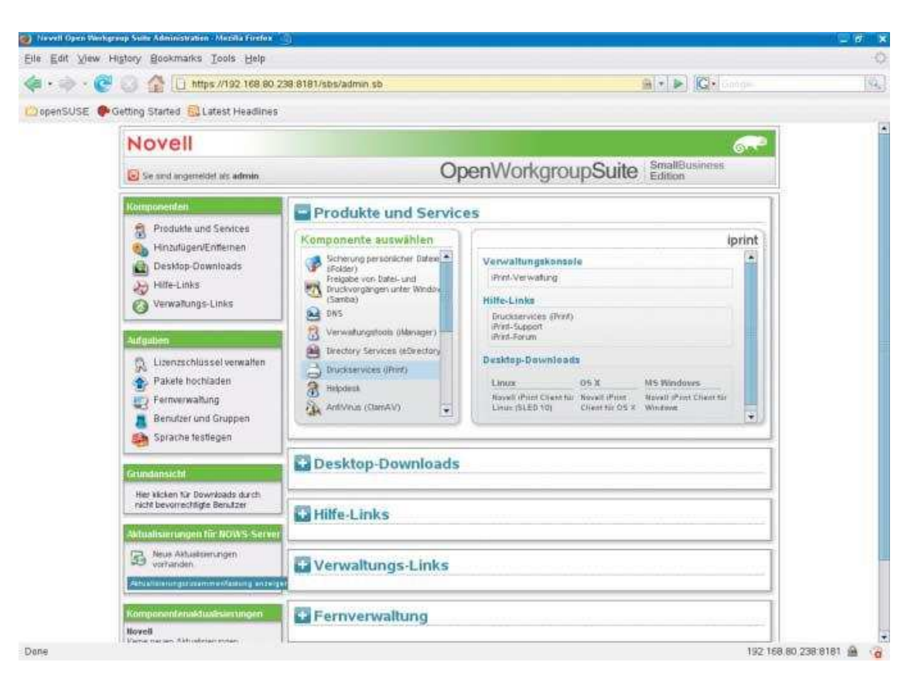
Xandros zeigt mit seinem Server einige sehr gute Ansätze. Insbesondere beweisen die Kanadier, dass man auch unter Linux eine Verwaltungsoberfläche schaffen kann, die sich im Handling selbst eingefleischten Windows-Administratoren erschließt. Leider lassen die Durchführung im Detail und die Stabilität derzeit noch zu wünschen übrig. Das größte Hindernis ist jedoch, dass der Systemverwalter mangels deutscher Lokalisierung der Kernelemente derzeit ohne (IT-)Englischkenntnisse nicht weiterkommt.



Novell Open Workgroup Server

Novell liefert mit dem Open Workgroup Server (NOWS) in der Small Business Edition eine auf dem SLES 9 (Suse Linux Enterprise Server) beruhende Software-Zusammenstellung, deren Verwaltung einheitlich über das webbasierte iManager-Tool erfolgt. Passend zum Server bietet der Hersteller mit dem Suse Linux Enterprise Desktop (SLED) einen Linux-Client an.

Die schon etwas angegraute SLES-9 Basis benutzt einen recht alten Kernel 2.6.5-7.286-default und setzt standardmäßig noch ReiserFS ein – angesichts der ungewissen Zukunft dieses Dateisystems eine eher unglückliche Wahl.



Für die Systemverwaltung setzt Novell ein Web-Frontend ein (Abb. 4).

Laut Hersteller arbeitet man an einer auf SLES-10 basierenden neuen Version. Kurioserweise warnt der Installer zwar, man sei gerade dabei, eine 32-Bit-Software auf einem 64-Bit-System zu installieren – es gibt jedoch gar keine 64-Bit-Version des Servers als Download (nur von den Clients). Für die Installation kommt Yast aus dem SLES zum Einsatz. Für Lesefaule kann sich dies rächen: Nur im Quickstart Guide (PDF) steht, dass man die Softwareauswahl während der Installation keinesfalls verändern darf. Im Installer selbst kann man dies jedoch einfach tun und es fehlt auch jeglicher Warnhinweis. Am Ende kopiert die Installationsroutine ungefragt den Inhalt der Installations-DVD auf die Festplatte. Das ist sicher hilfreich, wenn man ohne Einlegen der DVD später Software nachinstallieren möchte. Ob dies jedoch den Platzverbrauch rechtfertigt sei einmal dahingestellt.

Nach dem ersten Neustart läuft die Installation webbasiert weiter. Der modifizierte KDM-Login des Servers weist auf die URL der Admin-Oberfläche – allerdings in teilweise recht krausem Deutsch (siehe Abb. 3). Auch bei großen Firmen ist Lokalisierung ab und an Glücksache. Vor der Installation der weiteren Softwarepakete erfolgt erst einmal ein Online-Update (auf Wunsch), das im Test 26 Pakete umfasste. Danach stehen die zu installierenden Module zur Wahl: Das Spektrum reicht dabei von Dynamic Local User (legt auf angeschlossenen Windows-Clients automatisch den Nutzer an, sobald man ihn im eDirectory einträgt) über Directory Services (eDirectory) und Management Tools (iManager), bis hin zu VPN Server (OpenVPN) oder Firewall (IPTables). Die Auswahl ist umfassend, jedoch sind auch hier die Komponenten nicht unbedingt die neuesten. Zusätzlich zu einem TightVNC würde man sich ein (Free-)NX wünschen. Auch ClamAV ist sicher nicht der optimale Virenscanner – wenn auch der einzige kostenfreie.

Die Installationsprozedur hat durchaus noch ein paar Haken und Ösen: Zunächst startet sie wieder auf Englisch, selbst wenn man bei der Grundinstallation schon auf Deutsch umgestellt hatte. Außerdem muss man bei jedem Modul einzeln auswählen, ob man „basic“ oder „advanced“ wünscht – ohne weitere Erläuterung. Der Tester tappte auch prompt in eine Falle: Die Auswahl von „basic“ bei HylaFax führt zu einer Einrichtung des Faxservers für eine US-amerikanische Umgebung. Ebenfalls sollte man nicht versuchen, einen Faxserver auf einem Rechner ohne geeignete Schnittstelle einzurichten: die Installation hängte sich im Test einfach auf und präsentierte eine weiße Seite im Browser. Auch ein „zurück“ half nicht mehr; der Tester musste die gesamte Installation wiederholen. Auch am Samba-Paket verschluckte sich die Installation (eventuell als Folgefehler



Novell überrascht gelegentlich mit zumindest interpretationsfähigen Übersetzungen (Abb. 3).

der Fax-Panne) derart, dass das Einspielen (die Pakete liegen in */opt/media/nows/*) schließlich manuell mit *rpm -Uhv* … erfolgen musste .

Für die Administration bietet der NOWS eine komplett deutsch lokalisierte Weboberfläche. Sie ist recht komplex, aber auch vollständig. Leider ruft sie für fast alle Teilaufgaben in separaten Fenstern die Tools iManager oder iPrint auf – diese sind nur dann auf Deutsch, wenn der aufrufende Browser Deutsch als bevorzugte Sprache eingestellt hat, unabhängig von der Sprachwahl des Servers. Dem iManager merkt man die Herkunft aus der Welt der großen Rechenzentren an: Er kann alles und lehnt sich stark an die darunterliegenden eDirorectory/LDAP-Attribute an. Gut für den technisch versierten Administrator, aber schlecht für den aus der Windows-Welt kommenden EDV-Beauftragten einer kleinen Firma. Ohne technisches Wissen ist hier viel Handbuchlektüre nötig – die Oberfläche ist nicht intuitiv und besticht durch viele Abhängigkeiten: Einen Nutzer mit Homeverzeichnis kann der Administrator (logisch korrekt) erst anlegen, wenn er vorher die im Netz verteilbaren Speicherorte („Volumes“) eingerichtet hat. Einen Hinweis darauf oder auch nur einen Direktlink gibt es jedoch nicht. Wizards oder Assistenten, die den Administrator in der richtigen Reihenfolge durch den Dschungel führen, fehlen ebenfalls. Ob eine Administration auch über die Remote-Admin-Software ConsoleOne erfolgen kann, war nicht Gegenstand des Tests.

Novells Server für KMU stellt alle benötigten Dienste bereit. Man merkt ihm jedoch deutlich an, dass der Hersteller ihn aus großen Rechenzentrumsumgebungen abgeleitet hat. Die Bezeichnung „Small Business Edition“ bezieht sich augenscheinlich eher auf das Preismodell als auf die technische Konzeption – wofür auch die maximal zulässige Zahl von immerhin 200 Clients spricht. Für den Einsatz in kleinen Unternehmen eignet er sich nur, wenn ein technisch sehr versierter Mitarbeiter oder Dienstleister zur Verfügung steht. Novell teilte kurz vor Redaktionsschluss mit, dass die Veröffentlichung des auf SLES10 SP1 basierenden Nachfolgers kurz bevorsteht. Sobald er verfügbar ist, wird sich *iX* das Update noch einmal genauer ansehen.

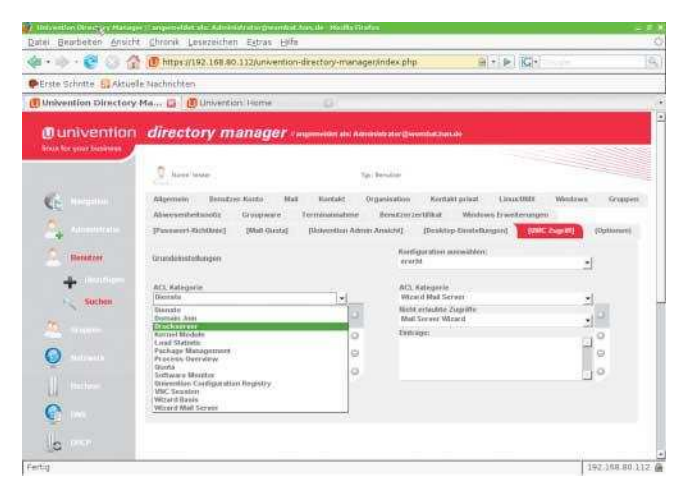


Univention Corporate Server

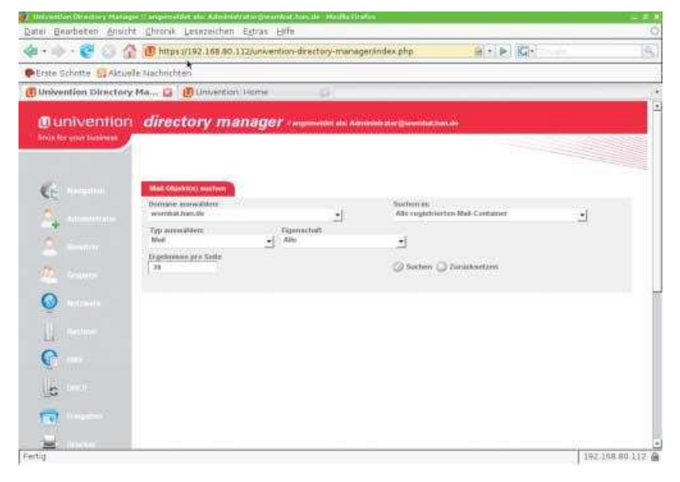
Eher am oberen Rand der Zielgruppe tummelt sich Univentions Corporate Server (UCS): Er lässt sich natürlich als alleinstehendes System einsetzen, aber seine besonderen Qualitäten spielt er in verteilten Umgebungen aus. Dort kann er dazu dienen, viele Server und Desktops zentral zu administrieren. Passend zum Server liefern die Bremer auch einen darauf abgestimmten Desktop. Wer zusätzlich zur normalen Serverfunktionalität auch eine Groupware wünscht, kann entweder den Univention Groupware Server (UGS) mit Kolab als Basis einsetzen oder den „normalen“ UCS mit zertifizierten Paketen wahlweise mit Kolab, Scalix oder Zarafa aufrüsten. Als Standarddatenbank ist PostgreSQL an Bord, allerdings nicht in die Administration eingebunden. „Spielereien“ sucht man vergebens, dafür ist – der Herkunft aus verteilten Umgebungen geschuldet – ein Nagios-Server mit an Bord.

Univentions Server basieren auf Debian (Kernel Version 2.6.18-ucs57, wahlweise auch 2.6.24). Nach dem üblichen Start eines englischen Grub schaltet die Installation auf Wunsch schnell komplett auf Deutsch um. Positiv ist, dass das System DNS- und LDAP-Domain-Angaben auf formale Konsistenz prüft – nicht jeder Vertipper führt so später zu schwer erkennbaren Fehlern. Außerdem akzeptiert UCS nur verhältnismäßig sichere Passwörter mit mindestens acht Zeichen. Als einziges Produkt im Test fordert der UCS die manuelle Eingabe aller Details (beispielsweise Länderkennung) für das generierte SSL-Zertifikat. Andere Produkte leiten diese Angaben aus anderen Eingaben ab oder verwenden Standardwerte.

Eine Virtualisierung mit Xen ist vorgesehen (nur mit dem 2.6.18er Kernel), der entsprechende Kernel wird mitinstalliert. Eine Einbindung in eine vorhandene DHCP-Struktur scheitert allerdings zunächst am nicht aktivierten DHCP-Client – eine manuell eingegebene statische IP ist Pflicht. Nach dem ersten Neustart präsentiert sich ein GDM X11 Loginscreen – den *root* allerdings nicht nutzen darf; der Superuser darf sich nur auf der Textkonsole einloggen. Der separat angelegte Nutzer „Administrator“ (ohne Root-Rechte) darf natürlich unter X11 ins System. Da die Administration jedoch komplett webbasiert ist, ist dies faktisch nie nötig – folgerichtig existieren keine über das normale Debian hinausgehenden grafischen Admin-Tools. Es existieren jedoch Konsolenwerkzeuge zur Administration, sodass sich UCS komplett mit Skripten steuern lässt und ohne X11 (der Server verwendet KDE) auskommen könnte.



Univentions webbasierter Directory Manager ist vielseitig und vollständig – auch wenn hin und wieder die Übersichtlichkeit ein wenig leidet (Abb. 5).



Für große Umgebungen sicherlich sinnvoll, im KMU-Sektor eher zu viel des Guten: Univentions obligatorische Suchmaske (Abb. 6).

Ein Hinweis auf die URL der Admin-Oberfläche fehlt jedoch auf dem X11-Loginscreen. An einer Stelle braucht man doch eine Shell: Die Lizenz lässt sich nur über ein Kommandozeilen-Tool einspielen. Die Weboberfläche ist in der verwendeten Standard-UGS-Installation nicht nur über HTTPS, sondern auch unverschlüsselt über HTTP zu erreichen – unter Sicherheitsgesichtspunkten keine sehr glückliche Idee. Über die integrierte Firewall lässt sich dies beheben. Im Gegensatz dazu verfällt eine geöffnete Admin-Session in der Weboberfläche schon nach fünf Minuten Inaktivität. Danach ist ein erneutes Einloggen erforderlich. Diese Einstellung kann man zwar ändern, muss dafür jedoch zunächst länger die Handbücher studieren. Da man nach einem neuen Login nicht wieder da landet, wo man aufgehört hat, sondern im Hauptmenü, lohnt sich diese Mühe jedoch.

Beim Test tauchte ein Lokalisierungsfehler auf der Textkonsole auf: Beim Einsatz von *latin1-nodeadkeys* erhält man trotz DE-Lokalisierung ein englisches Tastatur-Layout. Wählt man *latin1*, klappt alles wie erwartet. Diesen Fehler hat der Univention-Support als Bugreport aufgenommen, er dürfte in einer der nächsten Versionen wieder verschwunden sein. Außerdem trat ein Absturz der Webadministrations-Oberfläche auf, der wohl auf einem alten Debian-Paket beruht, das die *LOCALE* falsch setzt. Auch dies dürfte wohl bald beseitigt sein. Beide Anfragen bearbeiteten die Bremer sehr schnell.

Absolut vollständig ist die Weboberfläche zur UCS-Administration. Es lassen sich wirklich alle Details der verwalteten Dienste und Rechner einstellen. Da die Oberfläche kein Ajax einsetzt, funktioniert sie in allen Lebenslagen. Allerdings sieht sie schon etwas altbacken aus, vergleicht man sie mit den neueren Produkten. Ob man lieber „Web2.0“-Feeling oder etwas klassischeres mag, ist aber sowieso Geschmackssache. Weniger gelungen ist im Vergleich die Benutzerführung. Zwar existieren einige Assistenten für Routineaufgaben, die Oberfläche erliegt aber leider des Öfteren dem „Reiterwahn“ (siehe Abb. 5). Oft ist nicht ersichtlich, in welcher Reihenfolge man die Reiter beim Anlegen neuer Objekte abarbeitet. Das erfordert einige Einarbeitung.

Die gesamte Systemverwaltung beruht auf LDAP – der normale Administrator merkt davon jedoch nichts. Wer jedoch gerne direkt mit LDAP-Attributen jongliert, kann dies tun. Die Administration der Groupware ist bis hin zum Verwalten von Abwesenheitsnotizen komplett in die Oberfläche integriert – separate Tools sind nicht nötig. Der Fluch der Vollständigkeit zeigt sich beispielsweise bei der Samba-Verwaltung: Die Software bietet so viele Rechte-Einstellungen, dass die entsprechende Maske überladen wirkt. Dies ist jedoch nicht nur bei Univention so, auch die anderen Hersteller kämpfen mit diesem Phänomen. An manchen Stellen sind die Fehlermeldungen nicht besonders aussagekräftig: *“LDAP Fehler: Object class violation“* dürfte dem Admin in einem kleinen Betrieb nicht besonders helfen. Aber auch dies ist bei anderen Herstellern nicht besser. Eine Spezialität des UCS ist jedoch die unvermeidliche Suchmaske (siehe Abb. 6), die immer zu durchlaufen ist, bevor UCS irgendeine Liste (Nutzer, Drucker, Server, …) anzeigt. In großen Umgebungen sinnvoll – wenn jedoch nur ein einziger Server oder wenige Objekte vorhanden sind, stört es den Arbeitsfluss doch erheblich.

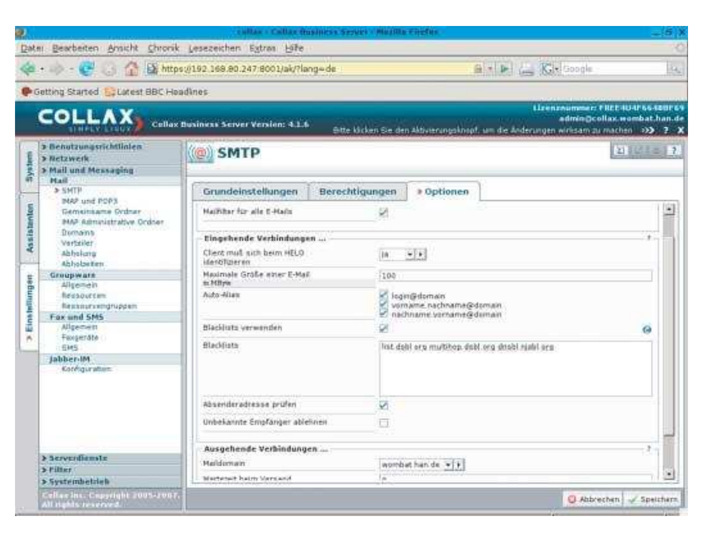
Auch als Einzelstück macht der inklusive aller Management-Werkzeuge unter der GPL lizenzierte UCS eine gute Figur – man merkt ihm jedoch an, dass er sich eigentlich gern mit mehreren seinesgleichen umgibt. Die rein webbasierte Administration ist vollständig, dadurch jedoch auch oft überladen. Eine Grundüberholung der Oberfläche in Struktur und Design würde dem Produkt sicher gut zu Gesicht stehen und ist laut Hersteller für Version 3.0 vorgesehen. Der Support des Bremer Herstellers ist dagegen gewohnt routiniert und schnell.

Collax Business Server

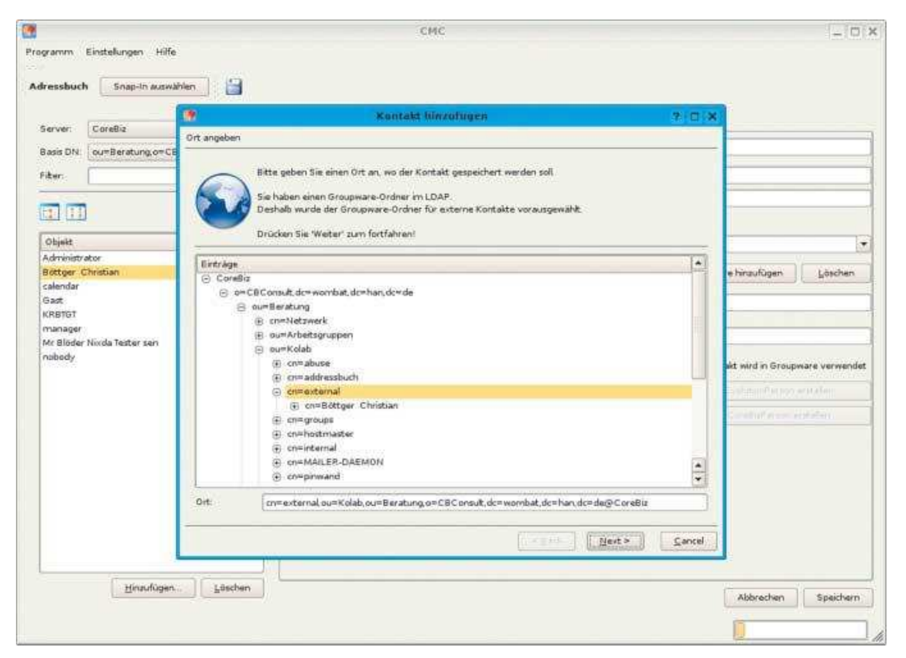
Collax zielt mit seinem Business Server bewusst auf kleinere und mittlere Unternehmen. Zur Erhöhung der Attraktivität bietet Collax eine ausführliche API an und ermuntert die Hersteller proprietärer Software, ihre Produkte für Collax zu portieren und anzubieten. Mit der Gewinnung von Pentaprise und Sage zeigt diese Strategie erste Erfolge. Den Collax Server gibt es als Business Server mit optionaler Groupware (Open-Xchange) oder als Collax OX-Server. Letzterer ist auf den Ersatz von Exchange fokussiert und bietet nicht alle Funktionen des Business Server. Alle Varianten bietet der Hersteller entweder als Software oder gebündelt mit Hardware als fertige Appliance an.

Installationspakete für den Server gibt es frei zum Herunterladen. Von der „LiveCD“ lässt sich das System auch installieren und betreiben. Für Aktualisierungen muss man eine bei Collax zu beziehende Lizenznummer eingeben. Weitere Module wie Virenscanner oder der Open-Xchange Server lassen sich durch die Eingabe weiterer kostenpflichtiger Lizenz-Codes freischalten.

Im hier betrachteten Umfeld eher ungewöhnlich ist die gänzlich textbasierte Installation. Dies ist grundsätzlich keine schlechte Idee, leider fehlt die Option, im Fehler- oder Vertippfall zum vorherigen Punkt zurückzukehren. Man sollte also nicht vorschnell *next* anwählen. Die Installationsroutine erfragt zwar die Zeitzone, nicht jedoch Sprache oder Tastaturbelegung. Das eigentliche Einspielen läuft auf *tty1*, auf *tty3* kann man den Fortschritt verfolgen. Interessanterweise befindet sich auf *tty4* eine offene Root-Konsole – dies ist bei keinem anderen System im Test so. Das auf der hauseigenen Linux-Distribution Pynix basierende System arbeitet mit



Dank AJAX bietet Collax eine optisch ansprechende Oberfläche, die sich vor allem für Linux-Unerfahrene eignet (Abb. 7).



Bei der CoreBiz Management Console schimmert das darunter werkelnde LDAP-Verzeichnis immer durch (Abb. 8).

Kernelversion 2.6.16.57 und verwendet eine proprietäre Oberfläche. Für den deutschen Markt fragwürdig ist, dass die angezeigte und zu bestätigende GPL (für die freien Teile) nur auf Englisch verfügbar ist. Nach dem ersten Neustart geht es nur per Browser (Port 8001) weiter: Collax installiert als einziges Produkt im Test kein GUI und hält den Plattenbedarf entsprechend klein.

Allerdings weist der Installationsprozess noch einige Merkwürdigkeiten auf. So legt er beispielsweise den *root*-Account an, das Passwort legt jedoch erst (als erster Schritt) nach dem Neustart die browserbasierte weitere Konfiguration fest. Letztere empfiehlt, dass *root*-Passwort „an einem sicheren Ort, zum Beispiel in einem Tresor“ (was gut ist) oder „besser in Ihrem Kopf“ aufzubewahren (was keine gute Idee ist, denn was passiert, wenn der Admin einmal krank wird oder kündigt?). Wenn man sich während der Basisinstallation vertippt, beispielsweise bei der Netzkonfiguration, und deshalb das System per Browser nicht erreichen kann, muss man zwangsweise ganz von vorne anfangen. Ein Beziehen der eigenen IP-Adresse per DHCP sieht Collax nicht vor, man muss für *eth0* eine feste IP einstellen. Das integrierte Open-Xchange geht anscheinend davon aus, in eine neue Umgebung zu kommen: Für die Groupware stehen keine Migrations-Tools zum Ersetzen eines Exchange-Servers bereit.

Da die Basisinstallation keinerlei Fragen zum Netz (außer Rechnernamen und Domainname) stellt, lässt sich die Installation entsprechend einfach bewerkstelligen. Die restlichen nötigen Parameter wie DNS-Server oder Default-Route trägt der Administrator später in der Weboberfläche ein; hier ist eine besser Benutzerführung möglich. Für die Grundkonfiguration durchläuft der Systemverwalter mehrere Assistenten, vorher ist der Server nicht wirklich betriebsbereit. Etwas Detailpflege an den Vorgaben würde dem Produkt guttun. Beispielsweise macht Collax bei der Einstellung eines externen NTP-Servers keinen Vorschlag, üblich sind bei anderen Produkten Vorschläge wie *pool.ntp.org* oder *ntp1.ptb.de*.

Im Test ließ sich zunächst nach der Installation keine Default-Route einstellen. Es gab zwar keine Fehlermeldung, aber auch keine Route. Der angefragte Support reagierte sehr schnell und stellte per Remote Login eine korrupte LDAP-Datenbank fest. Ein Recovery behob das Problem. Ungeklärt blieb jedoch die Ursache der Inkonsistenz.

Optisch präsentiert sich Collax mit moderner Ajax-Technik und lässt sich flüssig bedienen. An die Struktur muss man sich allerdings erst gewöhnen. Collax’ Besonderheit: Es führt Konfigurationsänderungen nicht sofort aus, sondern stellt sie zunächst in eine Warteschlange. Erst durch Anklicken eines „jetzt ausführen“-Knopfes landen die Änderungen tatsächlich im System. Hat sich viel angesammelt, kann das einige Zeit dauern. Im Prinzip ist dies eine gute Vorsorge gegen Vertipper, da man die Warteschlange bearbeiten kann. Da sich die komplette Konfiguration in einer Datei befindet, lassen sich im Support-Fall remote Konfigurationen erstellen und „am Stück“ einspielen. Ebenfalls lässt sich die Downtime eines Dienstes durch Zusammenfassen minimieren. Der Nachteil ist jedoch, dass der Administrator es leicht mal vergisst und die Änderungen eben nicht „scharf“ schaltet.

Alle nötigen Parameter lassen sich einstellen, bis hin zu Details des Mail- oder des mitgelieferten Jabber-Servers. Auch Auswertungen über den Systemzustand sind vorhanden, beispielsweise eine Grafik für den Plattenbelegungszustand. Aber auch hier treten gelegentlich noch kryptische Meldungen wie *“Error: code:500 origin:3“* auf.

Für die Ansprüche eines kleineren oder mittelgroßen Betriebs ist der Funktionsumfang völlig ausreichend, zumal mit Open-Xchange eine Groupware mit vielen Zusatzfunktionen wie Foren an Bord ist. Im Detail bemüht sich Collax um Vielseitigkeit: So lassen sich Dateibereiche (Shares) nicht nur über Samba (SMB/CIFS) und NFS zur Verfügung stellen, sondern auch via Apple-Filesharing, FTP und WebDAV. Der Mailserver lässt sich einfach, aber vollständig administrieren, bis hin zum Spamschutz, bei dem sich beispielsweise problemlos die bekannten Blacklists an- und abschalten lassen. Als Datenbank liefert Collax PostgreSQL und MySQL mit, nur Letzteres lässt sich jedoch über die Oberfläche administrieren. Die Steuerung einer USV ist genauso vorgesehen wie der Aufbau von IPSec-Tunneln oder die Netzüberwachung mit Nagios. Sogar einige Helferlein wie *ping* lassen sich über die Oberfläche nutzen.

Insgesamt hinterlässt Collax’ Business Server einen runden Eindruck. In die Oberfläche hat der Hersteller viel Arbeit und Liebe fürs Detail investiert, um sie auch auf Linux-unerfahrene Administratoren zu trimmen. Trotzdem fehlen keine wichtigen Details. Ungewöhnlich ist allerdings der Zwang, jede Änderung nochmals manuell aktivieren zu müssen. Es ist zu hoffen, dass Collax’ Bemühungen, weitere Anbieter von Anwendungssystemen für sich zu gewinnen, von Erfolg gekrönt werden.

CoreBiz Server

CoreBiz – der Linux-Server der Linux Information Systems AG (LIS AG) – ist in verschiedenen Ausführungen zu haben. Auf dem sogenannten Base Server

iX-Wertung

Collax
⊕ auch als Appliance erhältlich
⊕ umfangreiche Ausstattung
⊕ übersichtliche Administrationsoberfläche

⊖ Gefahr von Inkonsistenzen der Konfigurationsdatenbank
⊖ Schwächen im Sicherheitstest

CoreBiz
⊕ gute Projektunterstützung
⊕ hohe Sicherheit
⊕ automatische Installation

⊖ vergleichsweise spartanische Ausstattung
⊖ Administration sehr technisch

MS SBS
⊕ Integration der Komponenten
⊕ großer Funktionsumfang
⊕ gute Wizards
⊕ vertraute Benutzeroberfläche

⊖ nur maximal 75 Nutzer

NOWS
⊕ iManager sehr detailliert, aber unübersichtlich

⊖ alte Softwareversionen
⊖ unvollständige Lokalisierung
⊖ keine Wizards
⊖ schwere Mängel im Sicherheitstest

UCS
⊕ mehrere Groupware-Komponenten möglich
⊕ verteilte Umgebungen administrierbar
⊕ Xen integriert

⊖ detailverliebte, recht umständliche Administration
⊖ Schwächen im Sicherheitstest

Xandros
⊕ leichte Umgewöhnung von Windows
⊕ umfangreiche Ausstattung

⊖ keine deutsche Lokalisierung
⊖ Instabilität der Managementkonsole
⊖ erhebliche Mängel im Sicherheitstest

aufbauend gibt es Spezialisierungen für Backup, Terminalserver, Cluster, Storage, Firewall, EAI, Office, Client, CRM und Groupware. Für diesen Test kam die Groupware-Variante zum Einsatz, auf der ein Kolab werkelt. Die weiteren Module, darunter Backup und die Clusterfähigkeiten, waren nicht Teil dieses Tests.

Wer ein Produkt out of the Box erwartet, ist bei der LIS AG falsch, sie kümmert sich intensiv um ihre Kunden. Man kann den CoreBiz Server nicht „einfach so“ herunterladen. Jeder Kunde füllt zunächst einen Fragebogen zum gewünschten System aus, in dem er insbesondere die Netzumgebung festlegt. Die LIS AG prüft die vom Kunden gewünschte Konfiguration auf formale Konsistenz und hält im Zweifel Rücksprache. Als Ergebnis erhält man eine fertig vorkonfigurierte Systemumgebung auf DVD oder zum Download. Auf diese Weise braucht man bei der Installation nichts mehr einzugeben – man kann es aber auch nicht. Sollte doch ein Fehler passiert sein oder hat man etwas vergessen (beispielsweise eine ungewöhnliche oder kleinere Bildschirmauflösung als normal), muss die LIS AG zunächst ein neues Image konfektionieren.

Für die Installation setzt CoreBiz auf FAI (Fully Automatic Installation). Klappt alles, ist anschließend ein fertiges System einsatzbereit. Wenn nicht, muss man sich an den Hersteller wenden. Der Tester musste diesen Zyklus leider mehrfach durchlaufen: Beim ersten Versuch war die zugeschickte DVD schlicht defekt, beim zweiten Mal gab es einen Installationsfehler und erst im dritten Anlauf kam ein vollständig laufendes System am Ende heraus. Der Support durch LIS war jedoch immer sehr schnell und kompetent.

Technisch basiert CoreBiz auf Ubuntu 7.04 und nutzt die Kernel-Version 2.6.23-1. Damit verfügt es über die modernste Default-Kernel-Basis im Test. Als GUI nutzt es KDE, die Basisverwaltung kann über die normalen nutzerfreundlichen Ubuntu-Tools erfolgen.

Am wohlsten fühlt sich CoreBiz, wenn auch die Arbeitsplätze mit dem CoreBiz-Client ausgestattet sind. Für den Administrator bietet das einen angenehm einfachen Weg, die Arbeitsplätze zu installieren und zu administrieren. In der Verwaltungskonsole kann er die Rechner anlegen und ihre Attribute (bis hin zur Bildschirmauflösung) festlegen. Der in CoreBiz eingebaute PXE-Server stellt über einen TFTP-Server ein passendes Bootimage bereit. Hierfür verwendet er erweiterte DHCP-Attribute. Praktisch bedeutet dies, dass ein zu installierender Rechner nur noch ein PXE-fähiges Boot-ROM/BIOS braucht. Den Rest erledigt wiederum FAI. Andererseits bedeutet es, dass CoreBiz wegen der eigenen DHCP-Attribute zwangsweise einen DHCP-Server laufen lassen muss und sich nicht in eine bestehende DHCP-Struktur einpassen kann. Man muss den CoreBiz-Maschinen also mindestens ein eigenes Netzsegment spendieren, wenn man aus anderen Gründen schon einen DHCP-Server betreibt.

Für die Verwaltung der CoreBiz-Funktionsbereiche dient keine Weboberfläche, sondern ein eigenes GUI namens CMC (CoreBiz Management Console). Im Gegensatz zu den Management-Werkzeugen vieler Mitbewerber steht die CMC unter der GPL. Sie basiert auf dem grafischen LDAP-Verwaltungswerkzeug Luma, das auf SourceForge gehostet wird. Auch der Untertitel der CMC „LDAP Management made easy“ zeigt deutlich die Richtung: CoreBiz setzt auf LDAP zur Verwaltung. Dies merkt man dem Tool deutlich an: Immerhin drei der 13 Module des CMC beschäftigen sich direkt „roh“ mit der Verwaltung des LDAP-Baums (Schablonen, LDAP-Browser, LDAP-Suche). Auch in den anderen Modulen zeigt die CMC zumindest den Basis-DN immer an und verwendet ihn teilweise zur Selektion. Die CoreBiz-Verwaltung bewegt sich von allen getesteten Systemen noch am nächsten an der technischen Grundlage LDAP, die überall durchschimmert. Der Administrator tut also gut daran, sich in dieser Hinsicht eine gute Grundbildung zu verschaffen.

Im Gegensatz zu anderen Verwaltungsoberflächen wirkt die Oberfläche einfach gehalten und bietet keine Assistenten, keine Auswertungen, keine Statistiken. In der Groupware-Verwaltung beispielsweise lassen sich nur Ressourcen (im Kalender buchbar), Verteilerlisten und „Shared Folder“ verwalten, nicht jedoch beispielsweise der SMTP-Dienst oder Spamschutz. Unter Shared Folder versteht die CMC übrigens sowohl Dateibereiche als auch gemeinsame Kalender und Adressbücher. Aus LDAP-Sicht sicher richtig, aber nicht unbedingt der Denkweise des Nutzers angepasst. Und eben leider nicht vollständig in den Funktionen. Letzteres fiel beim Punkt „Datei- und Druckservice“ (Samba, CUPS) besonders unangenehm auf. Mangels mitgelieferter Druckertreiber ließ sich leider kein Drucker instal-

Daten und Preise

Produkt	Microsoft Small Business Server 2003 R2 Premium Edition	Collax Business Server	CoreBiz Server	Novell Open Workgroup Server Small Business Edition	Univention Corporate Server	Xandros Server 2
Hersteller	Microsoft	Collax	LIS AG	Novell	Univention	Xandros
WWW	www.microsoft.com	www.collax.com	www.lisag.de	www.novell.de	www.univention.de	de.xandros.com
Hardwarevoraussetzungen	512 MByte RAM, CPU ab 750 MHz, 16 GByte HD	512 MByte/1 GByte RAM, Pentium/Core2Duo CPU, 8/80 GByte HD (ohne/mit OX)	1 GByte RAM, Pentium-4- oder AMD64-CPU ab 2 GHz, 80 GByte HD, XGA-Grafik	512 MByte/1 GByte RAM, ab 450/700 MHz CPU, 6/10 GByte HD (32/64 Bit)	256 MByte RAM, Intel-kompatible CPU	512 MByte/2 GByte RAM, Pentium 4 oder besser, 40 GByte/120 GByte HD
Basis	Windows Server 2003	Pynix	Ubuntu	SLES9	Debian	Debian
Groupware	Exchange	Open-Xchange	Kolab	Groupwise	Kolab (Scalix, Zarafa)	Scalix
Webadmin	–	✓	–	✓	✓	–
Fileserver	SMB/CIFS Sharepoint (WebDAV)	SMB/CIFS, NFS, WebDAV, Apple FS, FTP, TFTP	SMB/CIFS, NFS	SMB/CIFS, NFS	SMB/CIFS, NFS	SMB/CIFS, NFS, FTP
Virenschutz	–	ClamAV, andere optional	ClamAV	ClamAV	ClamAV	–
Faxserver	✓	✓	–	✓	–	✓
Printserver	✓	✓	–	✓	✓	✓
DHCP + DNS	✓	✓	✓	✓	✓	✓
Datenbank	MS SQL	MySQL, PostgreSQL	–	MySQL	PostgreSQL	Oracle Express, MySQL Community
Directory-Server	ADS	LDAP, Samba	LDAP, Samba	eDirectory, Samba	LDAP, Samba	LDAP, Samba
Client-Verwaltung	✓	–	✓	–	✓	–
Zusatzsoftware	ISA Server, Sharepoint, Frontpage Business Intelligence Development Studio	WebDAV, Jabber, Apple Filesharing, IPSec, Nagios, NUT	Cluster, Backup, FAI-Client-Installation, PXE	OpenOffice.org, OpenVPN, Amanda, TightVNC, iFolder Backup, Helpdesk	Nagios, Xen, Heimdahl	Websphere Community, JBoss, NX, SugarCRM, Mambo, Forum, Wiki, Xen, O3Spaces
Preise	Server inkl. 5 Clients ab 750 €	Server inkl. 10 User ab 399 €/Jahr, OX-Modul 475 €/Jahr	Wartungsvertrag: 590 €/Jahr (25 User)	k. A., Produkt wird durch Nachfolger ersetzt	Server 290 €/Jahr, Management 30 €/Client+Jahr, Kolab 30 €/Client+Jahr	Server inkl. 5 Scalix- und Backup-Lizenzen ab 375 €

Alle Preise netto

lieren, da nicht einmal ein Postscript-Treiber auf dem System vorhanden war. Dies folgt wohl erst später. Die Dateifreigaben können per Samba oder NFS erfolgen, nicht jedoch per FTP, Apple Filesharing et cetera.

Allerdings muss man bei der Wichtung dieser Unvollständigkeiten beachten, dass die LIS AG ihre Kunden grundsätzlich im Rahmen von Projekten betreut. Es ist im Geschäftsmodell nicht unbedingt vorgesehen, dass man den Server nur (vorkonfektioniert) verkauft und der Kunde dann selber sehen muss, wie er damit zurechtkommt. Im Rahmen eines Implementierungsprojekts, und sei es noch so klein, kann der Hersteller natürlich solche Dinge ausgleichen und den Server an die Kundenbedürfnisse anpassen. Derzeit ist der CoreBiz Server weniger ein „Boxed Product“ als eine gute Basis für ein Implementierungs- und Beratungsprojekt.

Fazit

Linux glänzt durch Vielfalt. Das ist auch im Bereich der Server für kleinere und mittlere Unternehmen so. Die Ansätze sind durchaus verschieden – und damit die jeweilige Nische. Novell geht mit einem technisch komplexen Produkt, das sich eher in großen Umgebungen wohlfühlt, an den Start. Univention hat seine besonderen Stärken in verteilten Umgebungen. Xandros kümmert sich besonders um Windows-lastige Umgebungen und versucht, im Look & Feel dem Windows-Administrator entgegen zu kommen. Collax setzt auf ein Rundum-glücklich-Paket und die Hersteller von proprietärer Anwendungssoftware. Außerdem bietet es als einziger Hersteller in Eigenregie Appliances an. Die LIS AG dagegen tendiert eher zur Umsetzung im Projekt als zum Verkauf fertiger Boxen. Es ist für jeden Geschmack etwas dabei.

Bei den Oberflächen zeigt sich ebenfalls ein uneinheitliches Bild. Sowohl eigene GUIs sind im Einsatz als auch Weboberflächen mit verschiedener Technik. Bei den GUIs gewinnt Xandros – allerdings nur für Englisch sprechende Kunden. Bei den Weboberflächen sticht Collax heraus. In gewisser Weise stellt die CoreBiz Management Console den Gegenpol zum „Reiterwahn“ des Univention Corporate Servers dar: einfach, übersichtlich, aber leider auch nicht ganz vollständig. Irgendwo in der Mitte liegt wohl wie so oft die Wahrheit.

Leider gab es mehr Stabilitätsprobleme als erwartet. Meistens lag es an einem festgefahrenen LDAP, nur einmal versagte eine Datenbank. LDAP ist sicherlich technisch eine elegante Lösung, zum logischen Ordnen und Speichern von Konfigurationsdaten. Aber anscheinend ist OpenLDAP insbesondere bei harten Abstürzen des Rechners anfälliger für Inkonsistenzen und daraus resultierendes „Festfressen“ als es eine (echte) Datenbank (mit Transaktions-Engine) wäre – oder auch schlichte textbasierte Konfigurationsdateien. Allerdings waren im Test nicht alle Produkte betroffen, auch nicht alle LDAP-basierten. Die genauen Ursachen ließen sich nicht ermitteln. Nun, solange der Support des Herstellers sich schnell um solche Probleme kümmert, kann es dem Kunden letztendlich (fast) egal sein. (avr)

CHRISTIAN BÖTTGER

arbeitet als freiberuflicher IT-Berater und Projektmanager mit Schwerpunkt in den Bereichen Groupware, Projektmanagement und freie Software.

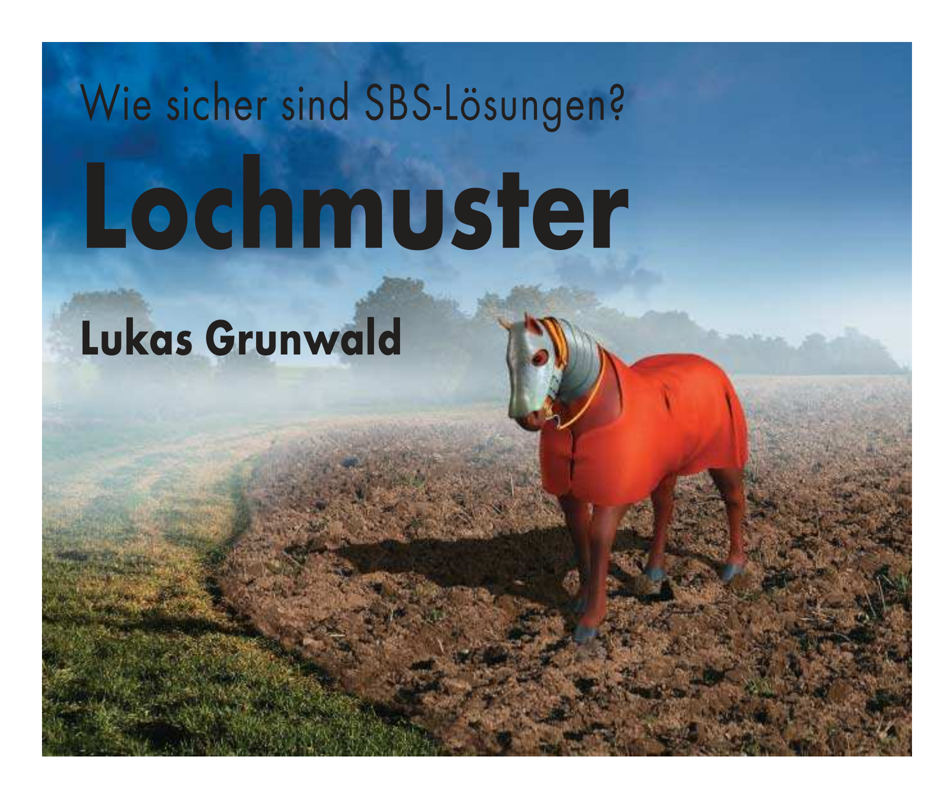
Literatur

[1] Lukas Grunwald; KMU-Server; Lochmuster; SBS-Lösungen in Punkto Sicherheit getestet; *iX* 6/2008, S. 62

[2] Christian Böttger, André von Raison; Groupware; Neu gruppiert; Collaboration-Lösungen für KMU; *iX* 5/2008, S. 99







Wie sicher sind SBS-Lösungen?

Lochmuster

Lukas Grunwald

Gerade kleinere Firmen haben oft weder das Geld noch intern das Know-how für ausgefeilte Sicherheitskonzepte. Wer meint, Out-of-the-box-Lösungen für diese Zielgruppe böten durchweg ein Mindestmaß an Systemsicherheit, irrt leider.

Gerade bei kleinen und mittleren Unternehmen (KMU) hapert es oft am Geld für ein Sicherheitskonzept oder gar ein Audit der eingesetzten Serverkomponenten. Klar ist, dass man bei dem Budget für die KMU-Server aus dem Artikel „Linux en miniature“ [1] keine hochsicheren Lösungen erwarten kann. Aber immerhin sollten sie nicht „gemeingefährlich“ sein und mindestens den Basis-Schutz einfacher Systeme liefern.

Daher mussten sich die Kandidaten einem Kurz-Audit unterziehen. Dabei schaute der Autor unter die virtuelle Haube der KMU-Server-Pakete und evaluierte, wie schnell ein Angreifer Administratorrechte auf den Systemen bekommen könnte.

Basiskriterien für Systemsicherheit

Auf Intrusion-Detection-Systeme (IDS) oder komplizierte Schutzmechanismen, die Kunden oft nicht bedienen können, sowie komplexe Logdaten-Korrelationen kann man bei KMU-Installationen verzichten. Hier ist in der Regel ohnehin kein fachkundiges Personal zu erwarten, das aus der Auswertung Kennzahlen und Trends extrahieren kann.

Umso mehr sollte aber die Basis des Betriebssystems sicher und einfach aufgebaut sein. Um das unter Beweis zu stellen, mussten die Systeme drei einfache Tests über sich ergehen lassen, wie sie jeder Unix-Administrator schon seit Jahren praktiziert.

Dateisystemberechtigungen: Hier stand die Suche nach gefährlichen Rechten wie SUID-Root-Flags und von jedermann beschreibbaren (sogenannte „World-Writeable-“) Dateien im Vordergrund. Dazu kamen die Tests aus dem Linux-Security-HOWTO von 2004 [2] – ein Klassiker, den die meisten Distributionen enthalten.

Software mit Schwachstellen: Eine Überprüfung des Versionsstandes der eingesetzten Software sollte klären, ob die Systeme gegebenenfalls Varianten mit Schwachstellen einsetzen. Da gerade im Linux-Kernel bis einschließlich Version 2.6.21 der IPv6-Stack ein potenzieller Einbruchskandidat ist, lief im Testnetz ein IPv6 Router Advertisement Daemon (*radvd*). Der verteilte ein IPv6-Präfix. Wenn ein System die angebotene IPv6-Adressen annahm, versuchte der Tester im Anschluss, die IPv6-Schwachstellen auszunutzen.

Netz-Bindung und *nmap*: Den Abschluss bildete ein Scan der Netzschnittstellen mit *nmap* – generell via IPv4, bei Systemen, die auf den *radvd* reagiert hatten, auch via IPv6. Dies lieferte die offenen Ports und weitere Details über die installierte Software. Der Aufruf *netstat -na | grep LISTEN* liefert zusätzlich Informationen darüber, ob die angebotenen Dienste auf allen Interfaces – „0.0.0.0:*“ oder im IPv6-Adressraum „:::*“ – horchen oder dediziert an IP-Adressen gebunden sind. Dies ist wichtig, da sonst bei der Installation einer weiteren Netzwerkkarte das System gegebenenfalls plötzlich die Dienste ungewollt auch darüber anbietet.

Microsoft Small Business Server

Da es bei Microsofts SBS wegen der Dateisystemberechtigungen schwieriger ist, das komplette System zu scannen, unterzog der Autor das System nur Tests mit *nmap* und dem GFI Languard, ein auf OVAL (Open Vulnerability and Assessment Language, oval.mitre.org) basierender Schwachstellen-Scanner. Dabei stellte sich heraus, dass die Frontpage-Extensions aktiviert sind – ein Sicherheitsrisiko für den Inhalt des Webservers. Auch sind Dienste wie NNTP und *snews* aktiv, die heute keinerlei Bedeutung mehr haben. Sonst ist keine aktuelle und akute sicherheitsrelevante Schwachstelle vorhanden.

Collax Business Server

Schon bei der Suche nach World-Writable-Dateien fällt auf, dass eine Squirrelmail-Installation mit beliebig ausführ- und schreibbaren PHP-Skripten auf dem System liegt. Dazu kommt, dass die verwendete Kernelversion (2.6.16.57) schon recht betagt ist. Immerhin hat Collax den IPv6-Support beim Bauen des Linux-Kernels ausgeklammert, sodass die Angriffe auf die aktuellen IPv6-Schwachstellen nicht greifen können. Das Argument Alter gilt auch für die Software-Pakete. Es bleibt allerdings unklar, ob die Entwickler die Sicherheits-Patches neuerer Versionen komplett zurückportiert haben. Immerhin gibt der Webserver keine Signatur aus.

Als nächster Patzer horchen alle Dienste global auf allen Adressen und Interfaces. Laut Hersteller kann man mit einer zusätzliche Firewall verhindern, dass das System die Dienste offen anbietet. Collax realisiert dies über einen via Webschnittstelle konfigurierbaren Paketfilter, der allerdings das Risiko in sich birgt, dass der Administrator sich selbst aussperrt. Change-Root, Jails, NTP und andere Sicherheitserweiterungen sucht man bei Collax vergeblich.



Univention Corporate Server

Nicht viel besser präsentiert sich Univentions Server UCS. Hier liegt der Windows-Installer für die Clients für jeden beschreibbar in */var/lib/univention-windows-installer*. Somit kann sich ein Angreifer auf dem Linux-System leicht die Kontrolle über die Windows-Clients verschaffen, da er in den Windows-Installer Trojaner-Funktionen einbauen kann.

Von der Netzseite her sieht es nicht besser aus: So verrät ein *nmap*-Scan genau die benutzte Software:

```
Apache httpd 2.2.3 ((Univention) PHP/5.2.0-8+ ↵
        etch 7.56.200712100724 mod_ssl/2.2.3 ↵
                              OpenSSL/0.9.8c)
Cyrus IMAP4 2.2.13-Debian-2.2.13-10.6.2007 ↵
                                    12032135
Samba smbd 3.X (workgroup: UCS)
```

Hier bekommt der Hacker Anhaltspunkte, welchen Exploit er anzuwenden hat, um in das System einzubrechen.

Selbst Debian installiert kein Telnet mehr und bindet den X11-Server auch nicht global an das Netz – UCS tut beides. Zwar ist der Telnet-Server kerberisiert, sodass die Passwortdaten nur bei abgelaufenem Kerberos-Ticket über das Netz gehen, und er erlaubt keinen Root-Zugriff. Dennoch ist ein Netzdienst mit Datenübertragung im Klartext immer ein Sicherheitsrisiko. X11 ließ sich beim Login via IPv6-Exploit remote über das Netz zum Absturz bringen. Außerdem horcht der UCS mit einem noch verwundbaren Kernel auf IPv6-Pakete im Netz, die verwendete Kernel-Version 2.16.18 besitzt hier noch Schwachstellen. Darüber hinaus binden sich die meisten Dienste an alle Interfaces.



Xandros Server

So mancher Mittelständler könnte sich wundern, wenn plötzlich die Polizei bei ihm klingelt und seinen Xandros-Server einsammelt. Hat er diesen direkt am Internet betrieben und als Proxy und Gateway benutzt, mag es der Anonymous-FTP-Server mit beschreibbarem *Incoming*-Verzeichnis gewesen sein, der so manchen Übeltäter im Internet dazu verleitet haben könnte, seinen Schmutz hochzuladen. Auch liegen im Filesystem liegen mehr als 1000 Dateien für jeden User schreibbar zum Manipulieren bereit, von Datenbanken bis zu PHP-Dateien, die besonders gefährdet sind.

Bei der Installation der Netzdienste macht Xandros den selben Fehler wie Univention: Alle genauen Software-Stände inklusive Patchlevel und Module lassen sich via Netzwerk anonym schnell herausfinden. Die Apache-Installation mit

```
Apache httpd 2.2.3 ((Debian) DAV/2 mod_jk/ ↵
        1.2.18 PHP/5.2.0-8+etch7 mod_ssl/2.2.3 ↵
      OpenSSL/0.9.8c mod_perl/2.0.2 Perl/v5.8.8)
```

reißt eine besonders kritische Stelle nach außen auf.

Auf IPv6-Adressvorschläge geht der Server gerne ein, mit seinem 2.6.18er-Kernel ist er hier voll verwundbar gegenüber den IPv6-Schwachstellen aus letzter Zeit.

Interessanterweise taucht beim IPv6-*nmap*-Scan ein neuer Service bei Port 9090 auf, der im IPv4-Netz nicht zu finden ist. Der Dienst fragt sofort nach den Superuser-Daten für einen nicht via IPv4 erreichbaren Blog. Ob es sich um ein „Osterei“ oder eine Schwachstelle handelt, muss sich noch herausstellen. Den globalen Netz-Interface-Bind hat Xandros genauso schlecht gelöst wie die anderen Distributionen.



Novell Open Workgroup Server

Es scheint, als wolle sich Novell mit seinem NOWS in der Small Business Edition um den Titel „Hackers Liebling“ bewerben. Schon beim Check der Dateisystemberechtigungen stehen einem die Haare zu Berge: Zahlreiche Dateien, darunter der Tomcat Applikationsserver sowie der iManager – das zentrale Verwaltungs-Tool von Novell – sind mit Schreibrechten für jeden versehen.

NOWS: Modifiziertes VPN-Skript

```
#!/bin/sh
# Physical address of device clients connect to
export SERVER_ADDR="192.168.80.238"
echo "roor::0:0:root:/root:/bin/bash" >> /etc/passwd
# Network to use for VPN
export VIRTUAL_RANGE="172.16.150.0"
# Network mask to use for VPN
export VIRTUAL_MASK="255.255.255.0"
```

Schlimmer noch: Auch Skripte, die der Webserver benutzt, sind es. So war es ohne Weiteres möglich, in das Environment-Skript von OpenVPN die Zeile *echo „roor::0…“* einzuschleusen (siehe Listing). Nachdem der Administrator dann das nächste Mal via Web die OpenVPN-Konfiguration aufgerufen hatte, existierten auf dem System plötzlich drei weitere Nutzer mit Root-Rechten – ohne Passwort.

So ein Patzer ist mehr als mangelhaft. Wenn Novell es nicht schafft, ihr Produkt sachgerecht zu prüfen, kann man niemandem raten, dieses System einzusetzen. Vom Hersteller hätte der Tester Besseres erwartet. Vielleicht sollte Novell erwägen, die Produktentwicklung nicht wie derzeit in den USA sondern vom hauseigenen Suse-Team in Nürnberg durchführen zu lassen. Dort arbeitet immerhin der eine oder andere Linux-Experte. Da hilft auch die Firewall nicht viel, die IPv6-Pakete gegenüber dem ebenfalls alten und anfälligen Kernel blockt.

CoreBiz Business Server

Am besten von allen Linux-Distributionen schnitt CoreBiz ab: Aktuelle und von Schwachstellen bereinigte Software bevölkert das System. Es traten weder Ungereimtheiten bei den Dateisystemberechtigungen auf noch gab es Schwierigkeiten mit den IPv6-Schwachstellen. CoreBiz setzt eine Kernel-Version ein, in der diese behoben sind.

Bei dem geänderten Root-Verzeichnis für den NFS-Server könnte sich so mancher Konkurrent von der LIS AG eine Scheibe abschneiden; hier haben die Berliner Entwickler etwas für die verbesserte Sicherheit getan.

Nur schafft es auch die LIS AG nicht, die Server-Signatur des Webservers so anonym einzustellen, dass der Apache nicht jede einzelne Version herausposaunt. Auch wenn die Module und der Server aktuell sind und keine Schwachstellen aufweisen, sollte sie hier ebenfalls die Server-Signatur abschalten.

Fazit

Bis auf Microsofts Small Business Server und CoreBiz von der LIS AG sind alle Systeme in der gestesteten Ausstattung sowie Konfiguration mit dem

betrachteten Release-Stand mehr oder weniger ein Sicherheitsrisiko. Man sollte sie „out of the box“ niemals am Internet betreiben, da potenzielle Angreifer in kurzer Zeit in die Rechner einbrechen können. Ein Härten, Verbessern und Einspielen von Sicherheits-Patches ist hier dringend angeraten. Die bequeme Zusammenstellung ersetzt keinen Administrator, und hinter der einfachen Oberfläche tun sich in Sicherheitsfragen oft Abgründe auf.

Wenn ein mit Root-Rechten laufender Java-Server-Pages-Server von allen schreibbare Skripte aufruft, zeigt das, dass der Distributionsbauer keine rechte Vorstellung von Linux- und Unix-Sicherheit hat. Hier hätte nach dem Zusammenstellen der Distribution ein Test nach dem „Linux Security HOWTO“ [2] so manchen Patzer verhindert. Dieser Artikel beschreibt den Stand vom 8. April 2008. Die Hersteller bekamen vor der Veröffentlichung die Gelegenheit, ihre Produkte zu aktualisieren. Ob sie davon Gebrauch gemacht haben, sollten potenzielle Kunden jedenfalls im Vorfeld einer Entscheidung überprüfen. Der Kasten „Herstellerreaktionen“ fasst einige Antworten zusammen. (avr)

LUKAS GRUNWALD

arbeitet als Consultant bei der DN Systems GmbH in Hildesheim und ist in diverse freie Softwareprojekte involviert.

Literatur

[1] Christian Böttger; Linux SBS; Linux en miniature; Arbeitspferde für kleinere Unternehmen; *iX* 6/2008, S. 48

[2] Linux Security HOWTO; tldp.org/HOWTO/Security-HOWTO/

Herstellerreaktionen

Vor allem zu den im Test aufgetretenen Sicherheitslücken respektive -schwachstellen gab es einige Rückmeldungen der betroffenen Hersteller. Es folgt eine Zusammenfassung der Angaben der jeweiligen Hersteller.

Univention

Ein inzwischen veröffentlichtes Sicherheits-Update behebt unter anderem die falschen Verzeichnisberechtigungen beim Windows-Installer. Darüber hinaus zwingt es den Administrator künftig, den Zugriff via HTTP statt HTTPS explizit zu bestätigen.

Versions-Strings der Dienste: Der Tester wirft dem Produkt vor, dass die enthaltenen Dienste Softwareversionsstände mitteilen. Dass die Programme dies tun, stimmt und wir halten das auch für richtig, weil „wohlwollende“ Client-Software daraus gegebenenfalls Rückschlüsse über Eigenschaften der Software ziehen und sich entsprechend verhalten kann. Unabhängig davon ist beim UCS allein schon durch den öffentlich zugänglichen Quellcode dokumentiert, welche Softwareversionen enthalten sind.

Was allerdings nicht stimmt ist die Behauptung, Angreifer könnten durch die zurückgegebene Versionsbezeichnung Rückschlüsse auf die enthaltenen Fehler ziehen. Insbesondere sicherheitsrelevante Patches liefern wir immer als Backport zu der in der entsprechenden UCS-Release enthaltenen Programmversion. Ein direkter Rückschluss auf Sicherheitslücken durch den Versions-String ist also nicht möglich.

Telnet: Den Telnet-Server nutzten bisher via UCS-gemanagte Thin Clients zum Initiieren von Sitzungen. Mittlerweile unterstützen die Thin Clients auch kerberisiertes SSH, sodass *ktelnet* nur noch für eine Übergangszeit mit installiert wird. Eine wirkliche Sicherheitslücke ist der Dienst unserer Ansicht nach aber nicht.

X11-Server: Wie im Hauptartikel schon angedeutet, benötigt UCS eigentlich keinen X-Server. Die Versionen vor UCS 2.0 verzichteten auf die standardmäßige X-Aktivierung. Im Small-Business-Umfeld war aber immer die erste Frage, wie man denn eine grafische Anmeldung einrichten könne, sodass wir uns nun mit UCS 2.0 dazu entschlossen haben, den X-Server standardmäßig zu aktivieren. Für Umgebungen, in denen eine hohe Sicherheit erforderlich ist, empfehlen wir die X11-Installation auf dem Server aber nicht.

Die Tatsache, dass der X-Server auch Remote-Verbindungen zulässt, ist dem Umstand geschuldet, dass in vielen UCD-Umgebungen (Univention Corporate Desktop) X-Programme auf unterschiedlichen Terminalservern ausgeführt und von einem (Thin) Client aus bedient werden. UCD verwendet hier heute dieselben Einstellungen wie eine auf UCS installierte X11-Umgebung. Wir werden zukünftig jedoch eine Konfiguration über das Managementsystem ermöglichen und die Voreinstellung so ändern, dass der Zugriff nicht erlaubt sein wird.

Bindung der Netzwerkdienste: Im Text heißt es, dass Netzdienste immer nur an ein Netz-Interface gebunden sein sollten, damit das System die Dienste nicht auch über eine beispielsweise neu eingebaute Netzwerkkarte anbietet. Unserer Erfahrung nach erwarten die meisten Administratoren das Gegenteil, nämlich, dass beim Einbau einer neuen Karte die Dienste ohne manuelle Einstellungen über alle Netzwerkinterfaces funktionieren. Wir haben uns deswegen für diesen Weg entschieden und halten dies auch nicht für sicherheitsrelevant, weil gerade im KMU-Umfeld SBS-Server, die nur auf bestimmten Interfaces bestimmte Dienste anbieten, nicht realistisch sind.

Kernel: Im Bereich der Kernel verfolgen wir folgende Strategie: Zu jeder UCS-Hauptversion gibt es einen Basiskernel, den wir über die gesamte Lebenszeit der Version mit Security-Updates versorgen. Im Fall von UCS 2.0 ist das Kernel 2.6.18. Da es aus technischen Gründen notwendig sein kann, neuere Kernels einzusetzen, stellen wir daneben immer wieder aktuelle Kernels für UCS bereit, so haben wir am 9.4.2008 Kernel 2.6.24 für UCS 2.0 veröffentlicht.

Collax

Kernel: Collax verwendet den sogenannten Bunk-Kernel. Der Kernel-Maintainer Adrian Bunk pflegt die Version 2.6.16 parallel zum aktuellen Kernel-Stream. Seine Zielsetzung ist, einen möglichst stabilen und sicheren Kernel zu gewährleisten. Aus unserer Erfahrung ist dieser Kernel sehr viel weniger anfällig gegenüber neuen Sicherheitslöchern. Den Bunk-Kernel bringen wir regelmäßig auf einen aktuellen Stand. Zum im Test erwähnten aktuellsten Kernel 2.6.23-1 trennen ihn 7 Tage von der Veröffentlichung.

Bindung der Netzwerkdienste: Alle Dienste sind durch die Firewall geschützt und horchen nur auf Anfragen aus Netzen, die der Administrator explizit zugelassen hat. Im Auslieferungszustand und auch nach dem Einschalten eines Dienstes ist dieser noch aus keinem Netz erreichbar. Erst wenn der Administrator einem Netz explizit die Berechtigung gibt, ist der Dienst erreichbar. Zudem lassen sich bestimmte Zugriffe aus dem Internet erst gar nicht einrichten. So ist es beispielsweise nicht möglich, den SMTP-Server aus dem Internet ohne Authentifizierung erreichbar einzurichten. Auch für den File-Server (*smb/cifs*) kann man die Firewall nicht für Anfragen aus dem Internet öffnen.

Dateiberechtigungen: Die world-writable SquirrelMail-Dateien sind korrigiert. Unsere Qualitätssicherung wird überprüfen, warum die falschen Berechtigungen bislang nicht entdeckt wurden. Insbesondere ärgerlich, dass „nur“, aber ausgerechnet die PHP-Dateien betroffen sind. Bei den einzelnen Paketen versuchen wir, einen vergleichbaren Ansatz wie Adrian Bunk zu fahren und lieber einen Back-Port statt einer neuen Version zu benutzen. Andererseits sind wir jedoch recht häufig gezwungen, auf aktuelle Versionen zu gehen.



Kommerzielle Virtualisierer: XenServer und Virtual Iron im Vergleich

Deckmäntel

Fred Hantelmann

Mit Citrix XenServer und Virtual Iron buhlen zwei Hersteller kommerzieller Virtualisierungsumgebungen um die Gunst der Kundschaft. Beide nutzen Xen als Grundlage und wollen mit ihren Produkten professionelle Anwender ansprechen. Messen lassen müssen sie sich am Branchenprimus VMware.

Komplette Distributionen mit dem Xen-3.1-Hypervisor, der Verwaltungsinstanz Dom0, einer integrierten API und grafischem Werkzeug zum Management bieten derzeit nur XenServer und Virtual Iron. Sie implementieren eigene Konzepte mit unterschiedlichen Leistungsmerkmalen: XenServer 4.1 nutzt eine 32-Bit-Dom0 auf Grundlage von CentOS 5.1 und für den Datenaustausch die Xen-API. Virtual Iron 4.2 hingegen verwendet eine 64-Bit-Dom0 aus Komponenten von SLES 10 SP1, bietet ein in Java geschriebenes GUI und implementiert zusätzlich Hochverfügbarkeit (HA) sowie eine Snapshot-Funktion.

XenServer bildet nur Teile seiner Funktionen über die GUI ab, erst auf der Kommandozeile kann der Anwender alle nutzen. Virtual Iron stellt das Management in den Mittelpunkt und geht direkt in den Ring gegen VMware: Gleiche Merkmale bei nur 30 % der Lizenzkosten, lautet das Versprechen der Softwareschmiede.

Beide Produkte sind nach 10 Minuten Installationsarbeit einsatzfähig. XenServer ist auf jedem Host der virtuellen Infrastruktur einzurichten; wahlweise von CD-ROM oder über das Netzwerk. Bei Virtual Iron reicht die Installation auf dem Managementserver. Von dort beziehen die Managed Hosts ihr Betriebssystem per PXEboot.

Windows 2000 SP4, Server 2003 (32- und 64-Bit-Version), XP SP2 und Vista (32-Bit) laufen auf XenServer und Virtual Iron vollvirtualisiert. Mitgelieferte paravirtualisierte (PV-) Treiber optimieren die Leistung der virtuellen I/O-Komponenten. Virtual Iron liefert Unterstützung für Vista 64-Bit und Windows Server 2008 in beiden Architekturbreiten. Da diese PV-Treiber nicht von den WHQL (Windows Hardware Quality Labs) signiert sind, verweigern neue 64-Bit-Windows-Versionen eine Installation.

Linux-Gäste kann der Anwender ab RHEL 4.x (32-Bit) und 5.x (32- und 64-Bit-Version) nebst seiner CentOS-Variante sowie SLES 9 und 10 SP1 einsetzen. XenSource nennt noch Kompatibilität mit Debian Etch und Sarge, den RHEL-Nachbauten von Oracle, Citrix' XenApp und Presentation Server, liefert aber nur dann Support, wenn Linux paravirtualisiert im Einsatz ist. Bei Virtual Iron läuft Linux stets vollvirtualisiert und die Kompatibilität schließt auch RHEL3 ein.

Weitere Hauptunterschiede: Gäste unter XenServer starten bei entsprechender Konfiguration automatisch nach Hochfahren des Hosts, können untereinander adapterlos per Ethernet kommunizieren, besitzen jeweils eigene und als Offset zur Systemzeit einstellbare Uhrzeiten, kennen aber keine Floppies. Virtual Iron liefert seinen Gästen auf Wunsch auch dieses Medium, wahlweise physisch oder als Netzwerk-Image aus dem Managementsystem heraus, kann Netzwerkkarten für Jumbo-Frames konfigurieren und Systeme mit integriertem Managementprozessor ein- und ausschalten. Anders als bei Xen-Vanilla kann ein Gast bei keinem der Produkte auf virtuelle SCSI-Festplatten zugreifen.



Citrix' XenServer

Auf seiner Homepage stellt Citrix den XenServer, derzeit in der Version 4.1.0, nach Registrierung als 296 MByte große ISO-Datei zum Download bereit. Wer Linux paravirtualisiert betreiben will, sollte sich zusätzlich das etwas kleinere Linux-Pack laden. Zwei als

Open Virtual Appliance (.ova) formatierte virtuelle Maschinen (VM) unter Linux stellt Citrix als Development Kit zusätzlich bereit: eins für Devices als ISO- und eins für Software als Zip-Datei. Die dazu verwendeten Open-Source-Komponenten der CentOS-Distribution kann man dort im Quellformat herunterladen.

Die kostenlose Express Edition des XenServer läuft auf Intel-kompatiblen 64-Bit-Systemen mit zwei Sockeln und maximal 4 GByte RAM. Sie unterstützt bis zu vier gleichzeitig aktive VMs. Wer mehr benötigt, muss entweder die Standard oder die Enterprise Edition lizenzieren, wahlweise als Jahresabonnement oder unbefristet. Beide sind auf Plattformen mit bis zu 32 Sockeln und 128 GByte RAM einsetzbar ohne Begrenzung der Zahl gleichzeitig aktiver VMs. Das Lizenzmodell gilt pro physischem Server.

Ab der Standard-Edition kann der Administrator mehrere Xen-Hosts parallel bedienen und außerdem virtuelle Netzwerkkarten mit VLAN-Tagging versehen. Die Enterprise Edition erweitert das noch um das Clustern gleichartiger Xen-Hosts in Ressourcengruppen (Pools), Shared Storage mit NFS über Fibre Channel, iSCSI oder NetApp Filer mit dem Betriebssystem Data ONTAP 7G und Life-Migration aktiver VMs zwischen Maschinen innerhalb eines Pools per XenMotion. Schließlich hat der Hersteller noch einen Quality of Service genannten Mechanismus implementiert, der auf lokalen oder per Host Bus Adapter (HBA) angeschlossenen Speichern im Logical Volume Manager (LVM) eine Priorisierung von Disk-I/O ermöglicht.

Die Steuerung der Hosts und darauf befindlicher VMs erfolgt wahlweise über die mitgelieferte grafische Windows-Anwendung XenCenter oder über das Kommandozeilenprogramm *xe*. Der Client *xe* kommuniziert über mehr als 250 Kommandos mit dem Xen-API-Agenten *xapi* eines Xen-Hosts und regelt das gesamte Management von Hypervisor und VMs. XenCenter nutzt ebenfalls die Xen-API, bietet aber bisher nur einen Auszug aus dem Sprachvorrat. Client und Server tauschen untereinander XML-RPC-Pakete aus, *xapi* archiviert sämtliche hostspezifischen Attribute in einer SQLite-Datenbasis, derzeit in der Version 3.

Vertraute Umgebung beim Installieren

Das Einrichten des XenServer, ob via CD/DVD oder über das Netz, ähnelt im Benutzerdialog dem von Red Hats Anaconda, entspringt aber einer Eigenentwicklung von XenSource, in Python gefertigt und analog zu Anaconda über das Paket *newt* gestaltet. Für ein unbeaufsichtigtes Kickstart-ähnliches Installieren muss der Admin das dazu benötigte „answerfile“ in XML-Notation kapseln. Insgesamt elf „Schlüssel“ stehen ihm zur Wahl.

Eine XenServer-Installation belegt stets den gesamten lokalen Plattenplatz des Host. Die ersten 4 GByte erzeugt das Einrichtungsprogramm als Systempartition, gefolgt von einer Backup-Partition gleicher Größe. Bei einem Update kopiert das Setup-Tool die Systempartition dorthin. Auf dem verbleibenden Bereich richtet es eine LVM-Gruppe ein, die Plattenplatz für lokale VMs reserviert. Sie bleibt bei einem Update erhalten, falls der Administrator sich dafür entscheidet.

In drei Schritten baut die Prozedur einen XenServer auf: Er partitioniert und formatiert die Festplatte, packt eine Reihe bzip2-komprimierter Tar-Archive aus und richtet den Bootloader *grub* ein. Beim ersten Neustart führt der XenServer Abschlussarbeiten durch, in denen er unter anderem die Grundkonfiguration der SQLite Datenbasis einrichtet. Anschließend kann sich der Administrator entweder auf der Konsole des Host anmelden oder mittels XenCenter eine Verbindung zum System herstellen. Falls vorhanden, muss er eine Lizenzdatei auf jeden Host als */etc/xensource/license* kopieren. Das gelingt entweder per *scp* oder über XenCenter.

Erste VMs kann er entweder am Host über die Kommandozeile oder bequemer Wizard-gestützt aus XenCenter heraus anlegen. Letztere Methode fragt nach der Auswahl eines Template, Namen für die VM, CD/DVD-Laufwerk oder ISO-Datei als Installationsmedium und Spezifikation der Hardwareausstattung. Das betrifft im Einzelnen die Zahl der CPUs (Windows maximal 8 Kerne, Linux bis 32), die RAM-Kapazität (bis 32 GByte), die Anzahl der virtuellen Festplatten (bis 8, CD-ROM zählt mit) und die Netzwerkkarten, von denen der Administrator in einem Gast bis zu 7 Stück konfigurieren kann. Sie dürfen aber auch komplett fehlen, was etwa den ressourcensparenden Betrieb einer Live-CD ermöglicht.

Nach dem Einspielen des Betriebssystems für eine VM muss die Integration der mitgelieferten XenServer-Tools folgen. Das sind paravirtuell arbeitende Gerätetreiber, die einerseits den Durchsatz im Bereich Netz- und Festplattenzugriff optimieren, andererseits dem XenCenter durchschnittliche Auslastungsdaten dieser Geräte plus der Speichernutzung der VM liefern. XenServer hält dazu eine ISO-Datei bereit, die der Anwender an den Gast einfach als CD/DVD-Laufwerk anbindet.

Linux-Gäste von der Konsole aus einrichten

Paravirtualisierte Linux-VMs installiert der Administrator vorzugsweise aus einem Netz-Repository, alternativ von einer CD-ROM oder einem ISO-Abbild. Das Einrichten erfolgt im Text-Modus, da Anaconda keine Grafikhardware erkennen kann. Nach dem anschließenden Hinzufügen der XenServer-Tools muss der Systemverwalter die Konfiguration des grafischen Display-Managers (GDM) modifizieren, damit der Gast statt *Xorg* standardmäßig den *Xvnc* für den Fernzugriff startet. Sämtliche Schritte und die Anpassung der Firewall beschreibt das 44-seitige Handbuch zur Gast-Installation.

iX-TRACT

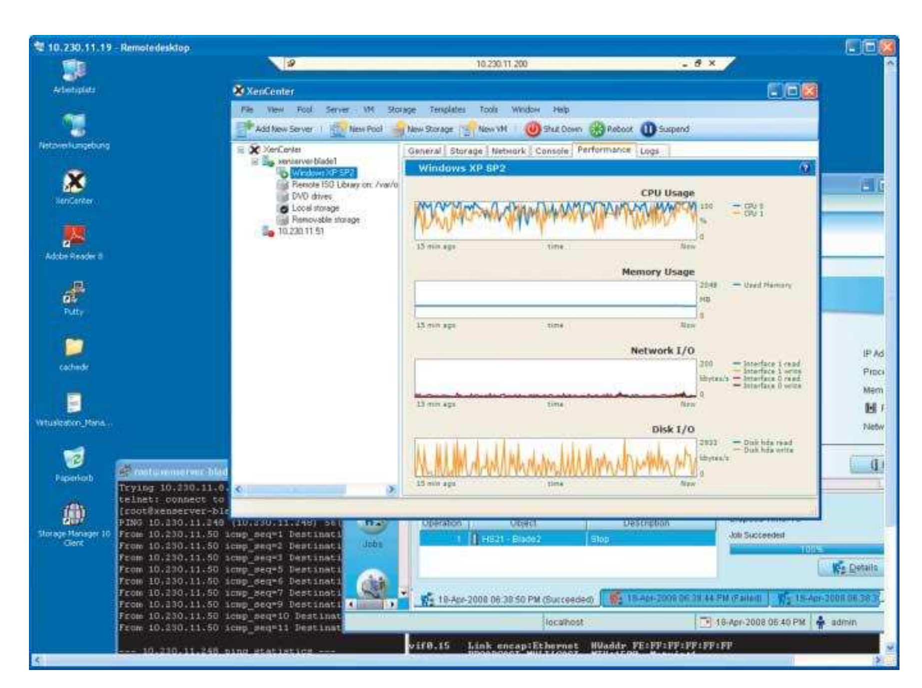
- Gegen den professionellen Einsatz von Xen als Virtualisierer sprach bisher die fehlende Administrationsoberfläche.
- Für den Einsatz im RZ bedarf es zudem einer professionellen Unterstützung.
- Zwei Produkte versuchen die Forderungen zu erfüllen: Virtual Iron und Citrix’ XenServer.
- Bei beiden handelt es sich um komplette Virtualisierungs-Umgebungen, die gegen VMware antreten wollen.

Im Test klappte es auch mit vollvirtualisierten Linux-VMs. Dazu liefert der Hersteller jedoch keine Tools, sodass außer für die CPUs die Performance-Daten für I/O und der VM-Speicherbedarf im XenCenter nicht sichtbar sind. Festplatten sind bei XenServer stets QEMU-IDE-Modelle, das CD-Laufwerk ist vom Typ QEMU-CD-ROM, und die Netzhardware reicht er als Realtek RTL-8139 durch. Übrigens gelang es, einen vollvirtualisierten RHEL-5.1-Clone aus den Sourcen zu erstellen. Das Ergebnis diente während des Tests zum Aufbau weiterer Linux-VMs.

Wer das Installieren der VMs aus ISO-Images bevorzugt, der kann für den XenServer ein lokales oder entferntes ISO-Repository anlegen. Von entfernten Systemen per NFS, CIFS oder SMBFS bereitgestellte Shares bindet das Kommando *xe-mount-iso-sr* an den XenServer-Host. Ein lokales Verzeichnis kann man zwar ebenfalls nutzen, aber die Autoren des Handbuchs stufen das wegen des knappen Plattenplatzes im Root-Dateisystem als riskant ein.

XenServer bindet virtuelle Netzwerkkarten über Bridges entweder an physische oder unterhält lokale adapterlose „Kommunikationspfosten“, über den die VMs eines Host untereinander Daten austauschen können. Optionales VLAN-Tagging erlaubt es, VMs in organisatorische Strukturen einzubetten, was der XenServer aber nur für virtuelle Schnittstellen unterstützt, die an eine Netzwerkhardware gekoppelt sind.

Virtuelle Festplatten erzeugt XenServer lokal oder remote als Images. Sie liegen entweder als Virtual Hard Disk (VHD) in Form einer Datei in einem lokalen oder per NFS gebundenen *ext3*-Filesystem, einer LVM-Partition oder einer LUN, die ein NetApp-Filer bereitstellt. Mit CD/DVD-ROM und USB-Geräten unterstützt XenServer zwei weitere Speichermedien, die er VMs als Hotplug-Devices liefern kann.



Huckepack: Virtual Iron auf Windows XP, gehostet von XenServer (Abb. 2)

VHDs erzeugt XenServer als Sparse-Datei, die nur den tatsächlich benötigten Plattenplatz belegt. Auf lokaler Harddisk richtet der Installer standardmäßig LVM ein, was der Administrator aber nachträglich ändern kann. Via Fibre Channel oder iSCSI gebundene Shared Storage Repositories müssen ebenfalls LVM-Gruppen und -Disks verwahren. Shared Storage bildet außerdem die Voraussetzung für XenMotion, da diese Funktion bei der Live-Migration nur das RAM-Image eines Gasts zwischen Systemen innerhalb eines Pools verschiebt, nicht aber seinen Plattenplatz.

Experimente mit Unterbrechungen

Das Anbinden über iSCSI unterstützt XenServer mit iSCSI-HBAs und einen im Produkt enthaltenen iSCSI-Software-Initiator. Der Übung halber exportierte ein Gast mit HVM-installiertem RHEL5-Clone ein iSCSI-Target an den betreuenden Host. Im Betrieb kam es jedoch zu empfindlichen Performanceeinbrüchen: Ein schlafender Vista-Gast auf demselben System benötigte mehr als 10 Stunden, um seinen 16 GByte großen Plattenplatz auf den iSCSI-Speicher zu kopieren. Die Prozedur dauerte 30 Minuten, wenn ein zweiter XenServer den iSCSI-Speicher vom ersten bezog und seinen lokalen Vista-Gast dorthin kopierte.

Schließlich geht es noch darum, wie XenServer mit FC-basiertem SAN zurechtkommen. Der Testaufbau bestand aus vier HS21-Blades von IBM mit integriertem ISP2422-Adapter von Qlogic. Drei waren in einem Pool gruppiert, auf dem vierten lief Windows XP. Er durfte mit XenCenter das Management für die komplette virtuelle Infrastruktur übernehmen. Als Zugang genügt ein PC mit Remote Desktop.

In dieser Umgebung startete das Einrichten eines Windows 2003 Server als VM, das der Tester mittendrin

unterbrach. Als er die Prozedur am nächsten Tag fortsetzte, kam sie ohne Störungen zum Ende. Anschließend ging es um die Migration der VM unter Last auf ein anderes System aus dem Pool. Zwischen ein und zwei der per *ping* ausgetauschten ICMP-Pakete gingen verloren, was auf eine Ausfallzeit von weniger als 2 Sekunden hindeutet. Das aber liegt innerhalb der zumutbaren Reaktionszeit und ist somit als Zero-Downtime akzeptabel.

Die zugänglichen Funktionen für Pool, Server, VM, Storage und Templates sind für die tägliche Arbeit ausreichend, decken aber, wie bereits gesagt, nicht das volle Leistungsspektrum der Xen-API ab. Performance- und Log-Informationen zeigt das GUI nur seit dem Öffnen einer Session an, und die Host- oder VM-spezifischen Daten gehen verloren, sowie der Anwender die Host-Verbindung schließt oder XenCenter beendet. Dringend sollte der Hersteller mindestens die Performancedaten in einer Datenbasis ablegen, sodass das Produkt Auslastungsstatistiken generieren kann. Das fehlt, wäre aber bei einem Produkt dieser Preisklasse eigentlich zu erwarten.

Virtual Iron

Der Zugriff auf Virtual Iron erfolgt analog zum XenServer über eine Registrierung auf der Webseite des Herstellers. Innerhalb einer Frist von 24 Stunden verspricht er die Zusendung einer Download-Adresse und eines Lizenzschlüssels mit 30-tägiger Gültigkeit. Das kann, wie im Test, länger dauern, da Virtual Iron seine Kunden nicht direkt bedient, sondern das von einem regionalen Vertriebler erledigen lässt. Im vorliegenden Fall hat die „Bearbeitung“ eine Woche gedauert. Die erste E-Mail enthielt URLs zum Zugriff auf die Virtual Iron Enterprise Edition 4.2.13 für Windows (164 MByte Install-Anywhere Exe), Linux (187 MByte Shell-Archiv) und einen Lizenzschlüssel für 20 Sockel, eine spätere alles für die Version 4.3.8.

Virtual Iron ist in zwei Versionen erhältlich: Die freie „Single Server Edition“ kann bis zu 12 VMs mit einer virtuellen CPU steuern und hält die Gast-Images auf der lokalen Festplatte. Die Obergrenze der Ausstattung liegt bei fünf virtuellen Netzwerkkarten und 15 virtuellen Festplatten pro Gast. In der pro Sockel lizenzierten „Extended Enterprise Edition“ (EE) lautet das Konzept „Bare Metal Virtualization“ unter anderem mit den Merkmalen virtuelles SMP (maximal acht pro Gast), Unterstützung von iSCSI- und FC-basiertem Shared Storage sowie VLAN. Des Weiteren sind Funktionen enthalten, die Virtual Iron LiveMigration, LiveMaintenance, LiveRecovery und LiveCapacity nennt. Obendrein bündelt er „EE“ mit dem LiveConvert genannten PowerConvert von PlateSpin und bringt pro Sockel sechs Lizenzen für Konvertierungen von Physical to Virtual (P2V) oder Virtual to Virtual (V2V) mit.

Der Einsatz von Virtual Iron EE setzt ein Managementsystem mit mindestens einer CPU, 2 GByte RAM, 30 GByte Plattenplatz und zwei Netzwerkports voraus. Die vollständig in Java geschriebene Oberfläche braucht mindestens JRE 1.5 und läuft auf RHEL 4 und SLES 9 in der 32-Bit- oder 64-Bit-Version sowie unter Windows Server 2003 (32-Bit). Im Test dienten RHEL 5.1 und Windows Server 2003 mit 2 GByte RAM als Grundlage für die Managementsoftware, die zur Laufzeit etwa 700 MByte beanspruchte.

Sogenannte „Managed Server“, auf deren Dienste die Steuerungssoftware zugreift, müssen Intels VT- oder AMDs V-CPUs enthalten. Dort zählen 2 GByte RAM, zwei Ethernet-Ports und laut Hersteller ein CD/DVD-Laufwerk vor Ort zur Mindestausstattung. Lokaler Plattenplatz zur Aufnahme von Hypervisor und den Dom0-Tools ist nicht erforderlich, da die Managed Server stets via PXE booten und die gesamte Software vom Managementsystem beziehen: Bare Metal Virtualisierung mit Xen 3.1, Suse Kernel 2.6.16 und 64-Bit-Dom0.

Bezug zum Installationspfad

Beim Einrichten der Software verlangt Virtual Iron eine gültige Lizenzdatei. DHCP aus den Cygwin Tools und alles Weitere liefert das Produkt mit und konfiguriert die Komponenten, während es den Managementserver installiert. Unter Windows richtet es einen neuen Service ein. Wer für seine

Management Host: Mindestanforderungen

Kategorie	XenCenter	VI Management Server	VMware VirtualCenter 2.5
Betriebssystem	Windows XP, Server 2003, Vista	RHEL 4.x, SLES 9, Windows Server 2003	Windows 2000 SP4, XP SP2, Server 2003
Runtime Environment	.NET framework version 2.0	JRE 1.5	.NET framework 2.0
CPU/MHz	eine, 750 MHz, 1 GHz empfohlen	eine; k. A.	eine, 2 GHz
RAM	1 GByte, 2 GByte empfohlen	2 GByte	2 GByte
Plattenplatz	100 MByte	30 GByte	560 MByte
NIC	einer, 100 MBit/s	zwei	einer, 100 MBit/s

Managed Node: Mindestanforderungen

Kategorie	XenEnterprise	Virtual Iron Enterprise Edition	VMware ESX 3.5
CPU	x64[1], 1,5 GHz	Intels VT, AMD-V	Intels Xeon, AMDs Opteron
RAM	1 GByte	2 GByte	1 GByte
CD-ROM	k. A.	ja	ja
HD local	PATA, SATA, SCSI ab 16 GByte	SATA, SCSI	SATA, SCSI
Shared Storage	FC-SAN, iSCSI, NFS	FC-SAN, iSCSI	FC-SAN, iSCSI, NFS
NIC	einer, 100 MBit/s	zwei	einer, 100 MBit/s

[1] Intel VT oder AMD-V für Windows-Gäste

Virtuelle Maschinen: Maximalausstattung

Kategorie	XenEnterprise	Virtual Iron Enterprise Edition	VMware VI 3.5 Enterprise
VCPUs	8/32[1]	8	4
VRAM	32/16 GByte [2]	64 GByte	64 GByte
VDisks	8	15	60
VCDs	1	1	4
VNICs	7[3]	5	4
VFloppies	–	1	2
Hotplug-VDisk	ja	nein	ja
Hotplug-VCD	ja	ja	ja
Hotplug-VNI	ja	nein	nein

[1] Linux-Gäste; [2] Linux Kernel 2.6; [3] drei für SLES 10 und RHEL 3, 4, 5

Managed-Server-Hardware spezielle Boot-Parameter benötigt, muss die Datei *default* unterhalb *bootfiles/microkernel/RELEASE/pxelinux.cfg* relativ zum Installationspfad ändern. Im Test war es auf einem System erforderlich, dem Linux-Kernel die Option *pci=nommconf* mitzugeben.

Das Sicherheitskonzept von Virtual Iron setzt eine Trennung von Management- und Produktivnetz voraus. Wer iSCSI nutzen möchte, muss dafür eine weitere Schnittstelle spendieren. Mindestanforderung an Massenspeicher ist laut Hersteller lokaler SATA-Plattenplatz. Damit sind aber Mehrwertfunktionen wie die Migration virtueller Maschinen nicht zugänglich.

Frische Massenspeicher erforderlich

Für Shared Storage unterstützt Virtual Iron iSCSI und FC-SAN, auf denen es jeweils LVM-Volumen einrichtet. Leider geht der Hersteller davon aus, „frische“ Hardware vorzufinden: Das Initiieren einer LUN im SAN schlägt fehl, wenn dort eine Volume Group vorhanden ist. Erst nach dem Löschen der Strukturinformationen kann das Management System die LUN in den gewünschten Grundzustand überführen. Virtual Iron nennt dieses Verhalten ein „Feature“, da die Software so vor dem Löschen von Fremddaten schütze. Statt eines passenden Hinweises terminiert dieser Job aber mit einer „internen“ Fehlermeldung.

Es reicht, wenn ein Managed Server innerhalb einer virtuellen Infrastruktur im Managementnetz integriert und BIOS-seitig für das Hochfahren über die betreffende Schnittstelle konfiguriert ist. Die Software erkennt die DHCP-Anfrage, generiert eine Kopie der PXEboot-Default-Datei mit seiner IP-Adresse gemäß DHCP-Lease in Hex-Notation und wartet auf die Bereitschaft eines Agenten im Server, der daraufhin die Gegenstelle zum Management bildet. Ein Login-Prompt stellt der Managed Server übrigens nicht bereit – einzig das Management System darf mit den Knoten Kontakt aufnehmen. Nachträgliche Änderungen an der Host-Hardware berücksichtigt das Management nach einem simplen „Rediscover“ des Host.

Von Hardwareherstellern mitgelieferte Managementmodule für das Intelligent Platform Management Interface (IPMI) oder HPs Integrated Lights-Out

(ILO) sind in das Produkt integriert. Damit soll der Anwender die Server über das GUI ein- und ausschalten können, nachdem man den Adressbereich der Baseboard Management Controllern (BMC) angepasst hat und im BIOS die im Managementnetz genutzte Maske gesetzt hat. Auf IBM HS21 gelang das im Test nicht, da die BMCs der Blades nur mit dem Management Modul des Bladecenter verbunden sind und keine Out-of-Band Steuerung unterstützt. Virtual Iron konnte die Serviceprozessoren erkennen, Ein-/Ausschalten per IPMI gelang aber nicht.

Erwartungsgemäß erfolgt das Konfigurieren der VMs per Wizard. Dabei kann man zunächst nur eine Netzwerkkarte und eine Plattenpartition angeben. Da eine erstmals konfigurierte VM aber nicht automatisch startet, kann der Administrator sie vorher seinen Wünschen entsprechend anpassen. Eine Boot-Reihenfolge gibt es für VMs nicht; es geht nur ein Medium: die Festplatte, ein lokales CD/DVD-Laufwerk, eine ISO-Datei auf dem Managementsystem als Networked Block Device (NBD) oder PXE. In der Regel ist nach dem Einrichten des Betriebssystems ein Umkonfigurieren erforderlich. Optimierte paravirtualisierte Treiber für 32- und 64-Bit-Windows (MSI) und -Linux (RHEL 3.x, 4.x, 5.x, SLES 9/10, RPM- und SRPM-Format) liefert der Hersteller als VS-Tools mit.

Die Managementoberfläche gliedert sich in Ressource Center, Hardware, Policies & Reports, Jobs und Users. Unter dem Punkt Hardware geht es um die Konfiguration von Netzen und Plattenpartitionen. Im Ressource Center gruppiert der Administrator die Hardwarekomponenten in Data Centern. Dort muss er VMs anlegen und kann die dafür gültigen Funktionen anwenden: Starten, Beenden, Konsole zur VM aktivieren, VM verschieben oder einen Snapshot erstellen. Ausgeschaltete VMs können als Vorlage für neue dienen; eine Clone-Funktion erzeugt ein Duplikat, was auch mit Snapshots geht, sodass indirekt das Clonen laufender VMs gelingt. Aktiviertes LiveRecovery erlaubt das automatische Verschieben, falls der beherbergende Knoten offline geht.

Berichtswesen mit Anhang

Im Bereich Policies & Reports verfügt der Systemverantwortliche insgesamt über 12 Arten von Berichtsgeneratoren, strukturiert nach Reports, User und System Policies. So erzeugt ein Node-Report zu jedem Managed Server Angaben über Zustand, vorhandenen und genutzten Speicher sowie die zugewiesenen VMS. Auslastungsstatistiken fehlen bisher. Als Grundlage der Reportgeneratoren fungieren Python-Scripte, die ein Wrapper mit den Java-Komponenten von Virtual Iron verbindet. Darüber greifen die Scripte auf die API des Produkts zu. Das soll Anwendern und Entwicklern einen Rahmen zum Aufbau eigener Anwendungen bieten. Siebzehn Pakete der API definieren stolze 520 Klassen.

Das Users-Menü schließlich regelt die lokalen Rechte der Benutzer, auf Wunsch mit Kopplung an einen LDAP-Server. Laut Hersteller kann der Administrator in einer nächsten Version des Produkts Rollen vergeben.

Zum Backup und Restore von VMs in Virtual Iron kann der Anwender VMs beziehungsweise Disk-Images von VMs im Format der Virtual Hard Disk (VHD) exportieren und entsprechend formatierte Images zurückladen. Das Produkt unterstützt ein dynamisches und ein festes VHD-Format. Zum anderen ermöglicht die GUI auf Knopfdruck eine Sicherung des gesamten Zustands der Konfigurations-Datenbank. Virtual Iron führt das per Default täglich durch und belegt pro Datensatz 30 MByte oder mehr. Die Zahl der maximal verwahrten Backups liegt bei 10, Rücksicherungen kann der Systemadministrator nur manuell ausführen.

Fazit

Virtual Iron und Citrix’ XenServer wollen die Ansprüche potenzieller Anwender mit eigenen Konzepten erfüllen: Virtual Iron darf als GUI-Sieger gelten, enthält HA- und Snapshot-Unterstützung, bringt IPMI- und ILO-Support mit – kann aber nur LVM-orientierten Plattenspeicher handhaben. XenServer muss im GUI-Umfeld nachlegen, bietet aber mit seiner konsequenten Client-Server-Architektur und der Xen API als Schnittstelle ein nahezu unbegrenztes Potenzial, wie es von heutiger Server-Virtualisierung zu erwarten ist.

Aufgrund fehlender Unterstützung für ältere Betriebssysteme wie Windows NT und dergleichen liegen die Vorteile der Produkte vordergründig im vereinfachten Zugang zur Virtualisierung mit Xen. Die beim nativen Xen enthaltene Unterstützung von logischen SCSI-Treibern für VMs fehlt. Vor allem die nicht vorhandene Langzeitarchivierung von Auslastungsstatistiken und Rollenstruktur für Administratoren zeigen, dass beide im direkten Vergleich mit den Produkten von VMware zurückstehen. (rh)

iX-Wertung

Citrix’ XenServer

⊕ voll- und paravirtualisierte Linux-VMs
⊕ Hotplug-USB-Disks und -Sticks
⊕ Import/Export von Open Virtual Appliance Images
⊖ eingeschränkte Verwaltung im GUI
⊖ Performancedaten zu grob und ohne DB-Unterstützung
⊖ keine Treiber-Tools für vollvirtualisiertes Linux

Virtual Iron

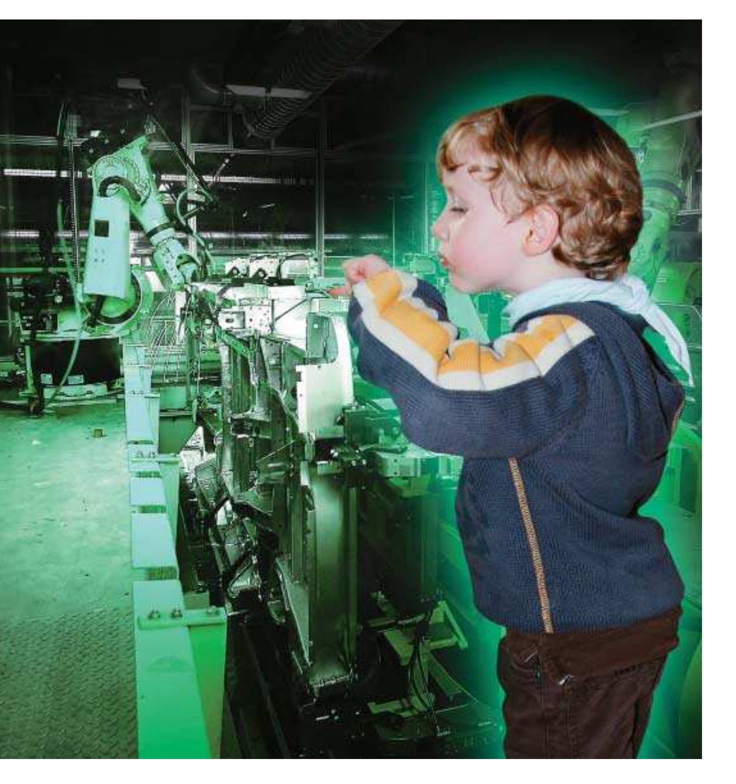
⊕ konsequente Out-Of-Band-Administration
⊕ Floppy-Unterstützung
⊕ zusätzliche Funktionen wie HA und Snapshot
⊕ Skripte für Reportgeneratoren
⊖ Performancedaten zu grob und ohne DB-Unterstützung
⊖ Lizenzierung nur über Vertretung vor Ort

FRED HANTELMANN

ist als IT-Architekt bei der Online Systemhaus ES+C GmbH tätig.

Literatur:

[1] Fred Hantelmann; Xen-Tutorial I; Xenologie; Aufbau virtueller Maschinen; *iX* 1/2007, S. 130
[2] Fred Hantelmann; Xen-Tutorial II; Phänomenologie; Konfiguration virtueller Maschinen; *iX* 2/2007, S. 129
[3] Fred Hantelmann; Core-Technik; Herzstück; Intels „Woodcrest“ mit Xen untersucht; *iX* 11/2006, S. 86



Metasploit 3.1

Gefährliche Experimente

Jörg Riether

Das Metasploit Framework erlaubt das gezielte Experimentieren mit den Schwachstellen von IT-Systemen. Mit Version 3.1 ist nun auch eine komfortable Windows-GUI-Version verfügbar, die es auch mäßig Informierten erlaubt, mit Sicherheitslücken zu experimentieren.

Die Zahl der Tools mit dem primären Fokus Schwachstellenentdeckung ist Legion. Die meisten haben eines gemeinsam: Sie informieren über gefundene Schwachstellen und teilen gegebenenfalls einen Weg zu deren Beseitigung mit – etwa das Einspielen von Patches. Worauf die meisten verzichten, ist das aktive Ausnutzen der Schwachstelle, etwa durch das Einschleusen einer Spionagesoftware.

Somit kann der Sicherheitsauditor den realen Angriff nur mit hohem Aufwand in der Praxis nachstellen – als Anhaltspunkte seien nur genannt die Exploitsuche im Internet, Kompilierung, die Analyse des Exploits, Auswahl eines möglichen nachzuladenden Schadprogramms (Payload). Genau hier setzt das Metasploit Framework an, eine freie Entwicklungs- und Angriffsumgebung, die im Juli 2003 H D Moore ins Leben rief. Moore, damals Direktor der Sicherheitsforschung bei Breakingpoint Systems, war es auch, der im Jahr 2006 das „Month of Browser Bugs“-Projekt (MoBB) startete. Ziel: Jeden Tag eine Browser-Verwundbarkeit veröffentlichen.

Überall zu Hause

Das Metasploit Framework läuft auf allen gängigen Betriebssystemen. Seit Version 3.0 wird es komplett in Ruby entwickelt (vorher in Perl). Die Bedienung lässt an Vielfalt kaum Wünsche offen; so kann man das Metasploit Framework sowohl über ein Konsolen-Interface nebst Tab-Komplettierung, über ein Ajax-veredeltes Webinterface, eine Gtk-GUI oder über das Scripting Interface auf der Kommandozeile komfortabel steuern. Die neue Version 3.1 bringt darüber hinaus ein echtes Schmankerl für die Windows-Benutzer, nämlich ein komfortables Windows-GUI.

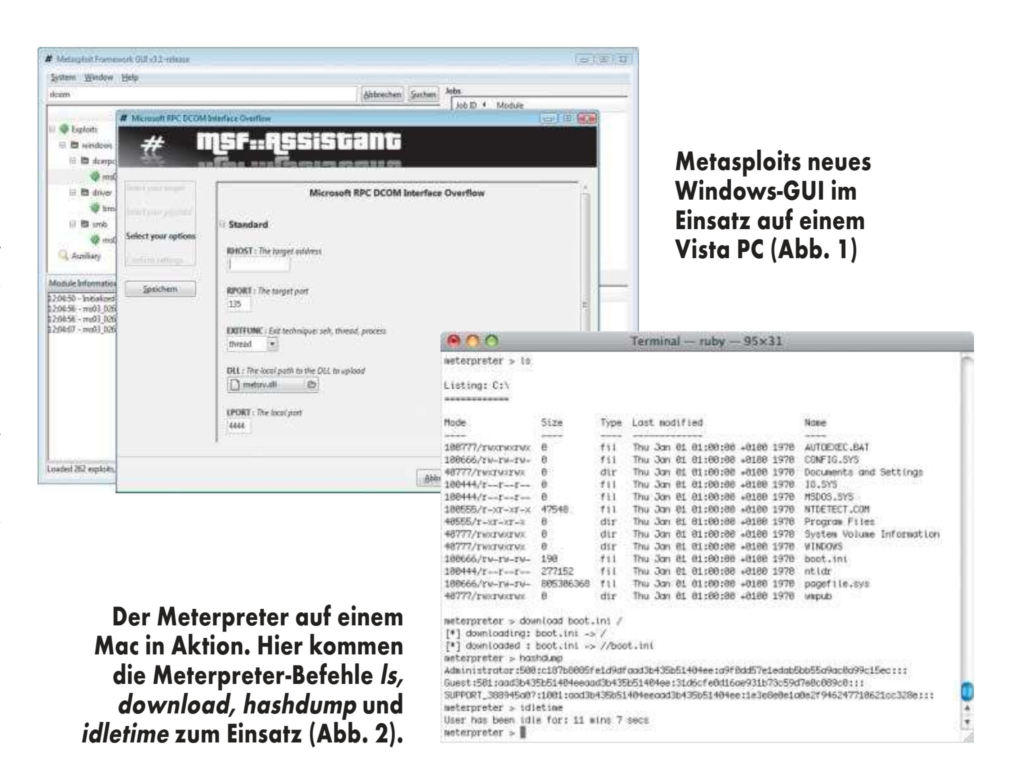
Ganz gleich, für welche der zahlreichen Bedienmöglichkeiten man sich entscheidet, ein typisches Angriffsprozedere läuft weitgehend gleich ab. Zunächst sucht man sich ein Angriffsziel und einen passenden Exploit. Insbesondere Letzteres lässt sich über eines der möglichen GUIs komfortabel mithilfe der Suchfunktionen erledigen. Die Anzahl der vorhandenen Exploits ist beachtlich und wird durch die interne Update-Funktion ständig erweitert. Zum aktuellen Zeitpunkt stellt das Framework über 260 Exploits zur Verfügung, für sämtliche gängigen Betriebssysteme, Applikationen und Hardware-Schwachstellen. Selektiert man einen potenziellen Exploit, zeigt einem Metasploit die verwundbaren Betriebssysteme samt Service-Pack-Level und gibt hilfreiche Informationen nebst weiterführender Links aus.

Als Nächstes wählt man das Angriffsziel, zum Beispiel Windows Server 2003 SPx. Darauf folgt die Wahl eines Payload, also der durch den Exploit übertragenen Malware. Auch hier hält das Framework eine Fülle von Möglichkeiten parat. Über 115 potenzielle Payloads, ebenfalls ständig über die Update-Funktion erweitert, stehen zur Auswahl bereit. An dieser Stelle kommt ein gewichtiges Feature des Metasploit Framework zum Einsatz. Allein anhand des gewählten Exploit vermag das Framework dem Nutzer automatisch die passenden Angriffsziele sowie die aktuell passenden Payloads zur Auswahl anzuzeigen. Ist zum Beispiel ein Payload zu groß für den zu beschreibenden Speicherbereich auf dem Angriffsziel oder gar nicht auf dem Zielsystem lauffähig, wird er ausgeblendet. Die Payloads gehen in Funktionsumfang und Vielfalt weit über die gängige BindShell (eine Kommandozeile auf dem Zielsystem) hinaus.

All diese Varianten im Detail zu beleuchten würde den Rahmen dieses Artikels sprengen, aber zumindest zwei wirklich beeindruckende Varianten sollen nicht unerwähnt bleiben.

Zum einen besteht die Möglichkeit, einen VNC-Server mit dem Payload *vncinject* nebst allen nötigen Parametern auf das Zielsystem zu laden und dort zu starten. Alles vollautomatisiert, versteht sich. Eine vor allem optisch sehr

beeindruckende Geschichte für Menschen, die der Aufklärung in puncto Trivialität eines erfolgreichen Angriffs bedürfen. Für den erfahrenen Angreifer hingegen stellt dieser Payload sicherlich nicht die erste Wahl dar, besteht doch die Gefahr, sehr schnell erkannt zu werden. Letzterer dürfte sich eher für die einfache Shell oder aber den Meterpreter, beeindruckende Variante Nummer zwei, entscheiden. Der Meterpreter wird später noch genauer beleuchtet; nur so viel vorab: Es handelt sich um einen extrem vielseitigen Payload mit nahezu unbegrenzten Möglichkeiten. Ist auch die Wahl des Payloads abgeschlossen, folgen letzte Konfigurationsschritte, Details der Ausführung des Angriffs betreffend.



Metasploits neues Windows-GUI im Einsatz auf einem Vista PC (Abb. 1)

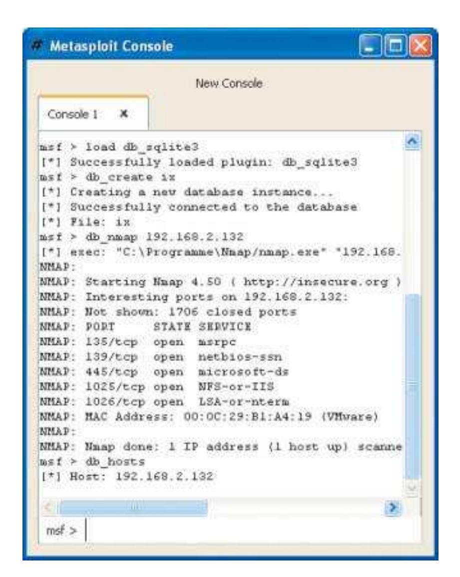
Der Meterpreter auf einem Mac in Aktion. Hier kommen die Meterpreter-Befehle *ls, download, hashdump* und *idletime* zum Einsatz (Abb. 2).

GUI für Ersttäter

Als wichtigster Punkt wäre hier das Ziel zu nennen, im Metasploit Framework „Remote Host“ (kurz RHOST) genannt. Der Zielport (RPORT) ist durch den Exploit vorgegeben, jedoch modifizierbar. Außerdem lassen sich unzählige Spezialparameter mitgeben, gegliedert in die drei Unterkategorien Standard, Advanced und Evasion. Nach den Pflichtangaben kann es mit dem Angriff losgehen.

Für erste Versuche empfiehlt sich das neue Windows-GUI. Es ist nicht nur übersichtlich und deckt trotzdem die komplette Feature-Vielfalt des Framework ab, sondern kann darüber hinaus in einigen Bereichen direkt mit dem Meterpreter interagieren.

Gewiefte Angreifer haben in der Regel ein Stück Software als Payload an der Hand, das bestimmte Aufgaben auf



Die Vorbereitungen für *db_autopwn* sind abgeschlossen (Abb. 3).



Nach einem Schuss ins Blaue auf ein ungepatchtes Windows 2003 mit *db_autopwn -t -p -e -s -b* steht sofort eine Session bereit (Abb. 4).

Onlinequellen

Metasploit-Homepage:
www.metasploit.com

Meterpreter-Referenz:
www.metasploit.com/documents/meterpreter.pdf

Metasploit Framework 3.1:
www.metasploit.com/framework

Benutzeranleitung:
www.metasploit.com/documents/users_guide.pdf

Entwickleranleitung:
www.metasploit.com/documents/developers_guide.pdf

dem Zielsystem erleichtert, sozusagen ein kleines Schweizer Taschenmesser. Der Meterpreter ist verglichen damit eine ganze Sammlung von Werkzeugkästen. Der enorme Unterschied ist schnell erklärt: Meterpreter kann live Erweiterungen nachladen, wodurch seine Einsatzszenarien nahezu unbegrenzt sind. Darüber hinaus laufen sowohl der Meterpreter selbst als auch seine Erweiterungen direkt im Speicher des Zielsystems und kommen nicht mit der Festplatte in Kontakt. Außerdem startet Meterpreter immer im Kontext der Anwendung, die die Schwachstelle aufweist, es wird also kein neuer Prozess auf dem Zielsystem gestartet.

Einige Erweiterungen liefert Meterpreter von Haus aus mit, zum Beispiel *fs*. Damit lassen sich beliebige Dateien vom oder auf das Ziel laden. Mit der Erweiterung *net* lassen sich unter anderem lokale Port-Weiterleitungen auf dem Opfer einrichten, die auf das Zielnetzwerk zielen und dem Angreifer das Tor zu internen Systemen öffnen, die er von draußen nie hätte erreichen können. In der aktuellen Version braucht man diese beiden Module nicht einmal von Hand nachzuladen, sie gehören jetzt zur *stdapi* und sind sofort verfügbar. Last but not least vermag Meterpreter seinen gesamten Netzverkehr zu verschlüsseln. Eine komplette Referenz des Meterpreters kann man sich auf der Metasploit-Homepage ansehen (siehe Links).

Mit Brute Force im Netz

Eines der wichtigsten, wenn auch nur mit größter Vorsicht zu benutzenden Features ist die Funkion *db_autopwn*. Dahinter verbirgt sich vereinfacht gesagt die Möglichkeit, eine Brute-Force-Attacke in Form aller passender Exploits des Metasploit Framework auf ein ganzes Netz vollautomatisiert loszulassen. Im Detail: Man untersuche mit *nmap* eines oder mehrere Angriffsziele auf offene Ports und die dahinter steckenden Anwendungen (nebst Version), schreibe diese Informationen in eine zuvor eingerichtete Datenbank und starte dann auf dieser Basis die passenden Exploits. Alles vollautomatisch, versteht sich.

db_autopwn tut genau dies. Diese Funktion ist deshalb so gefährlich, weil man damit zum einen einfach ins Blaue schießen kann, ohne sich auch nur ansatzweise mit der Auswahl eines Exploits beschäftigen zu müssen, zum anderen vermag *db_autopwn*, losgelassen auf ein großes Netzwerk mit vielen ungepatchten Maschinen, viele Systemabstürze oder Defekte hervorrufen. Der Sicherheitsauditor sollte also genau wissen, was er tut, oder sich warm anziehen.

Daten und Preise

Metasploit 3.1

Entwicklungs- und Angriffsumgebung

www.metasploit.com

Anbieter: community project managed by Metasploit LLC

Betriebssysteme: Windows, Mac OS X, Linux, Unixe

Fazit

Was in der Theorie manchmal abstrakt klingen mag, entpuppt sich spätestens dann als realistische Option, wenn man sich den Blog von Rise Security vom 08. Februar diesen Jahres ansieht (www.risesecurity.org/blog/entry/6/).

Die Gruppe hatte sich einen neuen Asus Eee PC angeschafft und quasi aus Spaß das Metasploit Framework darauf losgelassen. Schnell war klar, dass eine verwundbare Samba-Version installiert war, und wenige Sekunden später hatte man Root-Rechte auf dem Eee PC. Rise titelte „Asus Eee PC rooted out of the box“ und konkludierte süffisant: „Easy to learn, Easy to work, Easy to root“. Bei Asus dürfte das kaum jemand witzig gefunden haben.

Auch allgemein dürfte ein solches Zitat kaum Anlass zum Lachen geben, demonstriert es doch eindrucksvoll, wie trivial ein realer Angriff heute ablaufen kann. Die oder der verantwortungsvolle IT-Sicherheitsbeauftragte ist also gut beraten, sich mit dem Metasploit Framework einmal näher zu beschäftigen. Die Feature-Vielfalt ist beeindruckend, das Projekt wird ständig weiterentwickelt, hat eine starke Community und ist obendrein kostenlos. (JS)

JÖRG RIETHER

ist spezialisiert auf die Bereiche IT-Sicherheit, Hochverfügbarkeit und Virtualisierung. Er arbeitet als Abteilungsleiter der EDV bei der Zentrum für Soziale Psychiatrie Haina gGmbH.







Zukunftsaussichten: JDeveloper 11g Technology Preview

SOA-Bauklötze

Lars Niedermeier

Mit der 3. Technology Preview vom JDeveloper 11g gibt Oracle erstmalig Einblick in die nun integrierte Fusion SOA Suite 11g. Wichtigste technische Neuerung: Die Laufzeitumgebung basiert jetzt auf der Komponentenarchitekur SCA.

Wer mit dem JDeveloper 10.1.3 und der zugehörigen SOA Suite geschäftskritische serviceorientierte Anwendungen entwickelt, muss sich mit mannigfaltigen Infrastrukturfragen herumplagen. Er benötigt eine komplette Rechnerlandschaft bestehend aus mehreren Servern inklusive Softwarekomponenten wie Enterprise Service Bus (ESB), Application Server und Oracle-Datenbank.

Der JDeveloper 11g, derzeit in der 3. Technology Preview vorliegend, enthält nun die Laufzeitumgebung Fusion SOA Suite, ein Umstand, der dem Entwickler die Konzentration auf das Wesentliche erleichtern soll. Zum Beispiel kann er demnächst einen BPEL-Prozess (Business Process Execution Language) direkt in der IDE ausführen, das bislang notwendige Deployment auf dem Application Server entfällt. Zum endgültigen Release-Datum der elften Generation äußert sich Oracle nicht explizit, man kann aber davon ausgehen, dass sie Mitte des Jahres auf den Markt kommen wird.

JDeveloper 11g unterstützt alle gängigen Java-Standards wie JEE5, EJB 3.0 sowie JSF 1.2 und beherrscht das Editieren und Debuggen von Javascript. Ein UML-Modellierer ist jetzt integriert. Runderneuert hat Oracle das Application Developer Framework (ADF). Mithilfe des hauseigenen Open-Source-Produkts entstehen zum Beispiel die GUIs (Rich-Web-Clients) der Fusion-Anwendungen. Zudem kommt ADF bei Infrastruktursoftware wie der Enterprise Manager Fusion Middleware Console sowie intern eingesetzten Applikationen zum Einsatz.

Mit ADF Faces und dem auf Java Server Faces (JSF) basierten ADF Controller Framework lassen sich deklarativ Rich-Client-Webanwendungen entwickeln, die entweder als eigenständige JEE-Programme laufen oder in die SOA-Suite integriert werden, etwa als „Human Tasks“, Teilprozesse, die menschliche Interaktion erfordern. Für Ajax-Entwickler steht eine Komponentenbibliothek bereit.

Web 2.0 im Unternehmenseinsatz

Oracles Produktstrategen glauben, dass das sogenannte Social Computing (Wikis, Portale) im Unternehmen immer mehr Bedeutung gewinnt und haben deshalb das hierfür zuständige Web Center in 11g eingebaut. Nun kann der Entwickler mit dem JDeveloper entsprechende Intranet-Anwendungen bauen. Zu beachten dabei: Ajax und Co. in 11g verlangen mindestens Version 7 des Internet Explorer oder Firefox 2.0.02, ansonsten zeigen sie die Seiten der neuen Rich Clients nicht an.

Interessierte können sich die JDeveloper-Preview im OTN als Build-Version 4796 herunterladen. Das 769 MByte große Archiv für Windows enthält bereits das notwendige JDK 5, die Linux-Variante nicht. Wer keine 10g-Datenbank im Einsatz hat, auf die er als *sysdba* zugreifen darf, muss noch 10g XE installieren (alle Downloads sind über den *iX*-Link am Ende des Textes erreichbar).

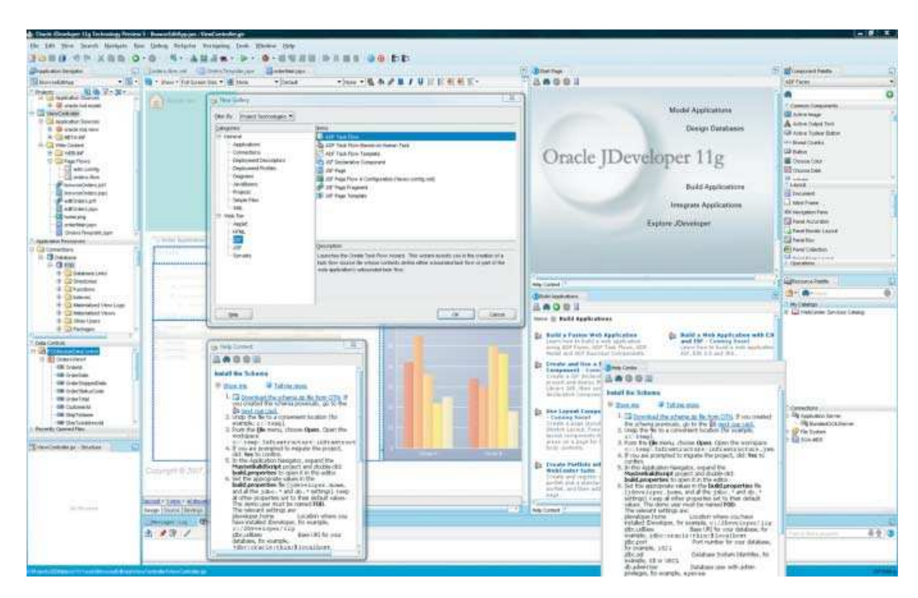
Als Testrechner dienten verschiedene Notebooks (Intel Pentium 1 GByte RAM bis Intel 64-Bit Dual Core, 2 GByte RAM) sowie einen Server mit Dual Core Athlons von AMD mit 4 GByte Speicher und Virtualisierung unter XenV3 beziehungsweise OracleVM. Die verwendeten Betriebssysteme waren Windows XP, Vista Ultimate, Opensuse 10.3, Red Hat Enterprise Server 4 sowie Oracles Enterprise Linux 5 Update 1. Letzteres lief sogar als para-virtualisierte Guest-Domain unter OracleVM für die Oracle-XE-Datenbank, JDeveloper und die SOA Suite. Die empfohlenen 2 GByte RAM erwiesen sich als absolut notwendig.

Sowohl unter Windows als auch unter Linux ist die Installation nach

wenigen Minuten abgeschlossen. Lediglich veraltete JDKs zwangen sporadisch zur Fehlersuche. Mit dem folgenden Linux-Befehl lässt sich die Version und der Installationsort des JDK ermitteln: *# rpm -q jdk -i -l | head -30*. Als weitere Hürden vor dem Einsatz können sich die schiere Masse an Informationen vom OTN sowie die nicht immer nachvollziehbaren Änderungen an den Webseiten erweisen.

JDeveloper begrüßt den Anwender mit einer in fünf Rubriken gegliederten Startseite. Mittels Klick auf *Build Applications* gelangt man zum mehrteiligen Tutorial *Build a Fusion Web Application*, das ADF Faces, ADF Task Flows und ADF Business Components behandelt. Die einzelnen Schritte veranschaulicht eine sogenannte Cue Card, eine Hinweiskarte, die man als eine Mischung aus Onlinehilfe und Wizzard beschreiben kann. Sie lässt sich frei in der IDE platzieren und klont sich bei einem modalen Dialog selbst in einen Child-Dialog, der nie verdeckt wird.

Falls die Hinweise der Cue Card nicht ausreichen, kann der Entwickler über den Hyperlink *Tell me more (what I see in the IDE)* weitere Details abrufen. Wichtige Schritte sind ebenfalls mit Hyperlinks unterlegt, sodass er den Befehl direkt ausführen kann und nicht erst lange in der IDE suchen muss (Abb. 1). Eine funktionsfähige Infrastruktur vorausgesetzt, benötigt man für das Erstellen der Fusion-Anwendung *BrowseEditApp* nur 20 Minuten.



So präsentiert sich der JDeveloper 11g unter Vista Ultimate bei der Entwicklung mit ADF. Im Vordergrund sieht man die Cue Card (Abb. 1).

Manuelle Kodierung auf dem Rückzug

Positiv fällt auf, dass sich alle relevanten Teilschritte einzeln ausführen und testen lassen. Die Programmierung erfolgt hauptsächlich deklarativ (Ausfüllen von Dialogen, Drag & Drop, kein Java-Coding), wie man es aus Siebel-Werkzeugen kennt. Ebenfalls aus dem Siebel-System hat Oracle die Konzepte LOV (List-of-Values) und Business Component übernommen. Siebel CRM wird mit der nächsten Release 8.1 erstmalig ADF einsetzen. Dass sich grafische Auswertungswerkzeuge für Systemdaten (Transaktionen und Ähnliches) leicht einbinden lassen, ist ebenfalls angenehm. Neben dem im Tutorial verwendeten Balkendiagramm existieren über 20 weitere Diagrammtypen.

Das 590 Seiten umfassende PDF-Dokument „Web User Interface Developers Guide for Oracle Application Development Framework 11g“ (im Installationsumfang enthalten) und die Online-Dokumentation der ADF Faces Rich Client Tags beschreiben die Möglichkeiten von ADF. Zur Vertiefung liefert Oracle den 1250 Seiten starken PDF-Wälzer „Fusion Developers Guide for Oracle ADF 11g“. Er beschreibt beispielsweise, wie man komplexe ADF Task Flows erstellt, die mit einem BPEL-Prozess interagieren.

Peoplesoft, JD Edwards und Siebel, die zugekauften ERP- und CRM-Produkte, sollen in den Fusion Applications aufgehen. Laut Oracle kommen die ersten in diesem Jahr auf den Markt. Peoplesoft CRM verwendet intern bereits mit dem Release 9 den BPEL Process Manager sowie Business Activity Monitoring von Fusion.

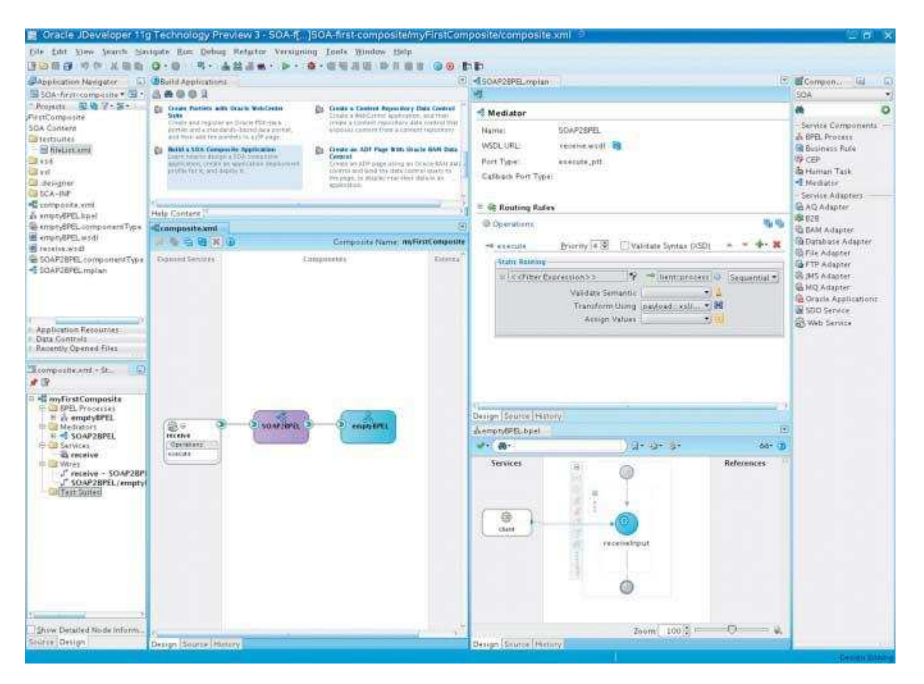
Neue Basis: Komponentenmodell SCA

Die wichtigste technische Umstellung ist die auf den OASIS-Standard SCA, (Service Component Architecture) [1]. Dabei handelt es sich um ein Komponentenmodell für serviceorientierte Anwendungen, die aus sogenannten Composites zusammengebaut werden. Sie sind die kleinsten Deployment Units. Eine SOA Composite setzt sich aus verschiedenen Components zusammen. Das können BPEL-Prozesse, Human Workflows, Business Rules oder das im Oracle-Jargon „Mediator“ genannte ESB Routing sein. Mit dem Composite-Editor führt der Entwickler die Teile zusammen (Abb. 2). Das Ergebnis ähnelt einem Schaltplan für digitale Bauelemente. Neben SCA unterstützt 11g BPEL 2.0 sowie die Standards WS-ReliableMessaging, WS-PolicyAttachment, WS-MetadataExchange und WS-SecurityPolicy.

Für den schnellen Einstieg bietet 11g das auf Cue Cards basierende „Build a SOA Composite Application“. Oracle verspricht Upgrade-Pfade für die Vorgängerprojekte – entweder interaktiv über JDeveloper oder per Kommandozeile für den Batch-Betrieb. Die über 1000 Seiten umfassende „Einführung“ in die SOA-Suite und SCA beschreibt

iX-TRACT

- Oracles Entwicklungssystem JDeveloper 11g enthält die bislang eigenständige Laufzeitumgebung SOA Suite.
- In der nächsten Generation stellt Oracle sein Fusion-Softwaresystem auf die von OASIS standardisierte Komponentenarchitektur SCA um.
- Noch in diesem Jahr sollen die ersten Fusion-Anwendungen das Licht der Welt erblicken. Sie enthalten alle Merkmale der ERP- und CRM-Produkte von Siebel, JD Edwards und Peoplesoft.



JDeveloper vereint die verschiedenen Elemente einer SOA Composite-Anwendung (wie BPEL-Prozess, ESB Mediator, Webservice-Interface) unter einer Oberfläche (Abb. 2).

detailliert die Umsetzung der Komponentenarchitektur sowie die Interoperabilität der SOA-Suite mit anderen hauseigenen Produkten.

11g soll Unternehmen in Lage versetzen, SOA inkrementell einzuführen. Bei komplizierten und langlebigen Prozessen kommt BPEL zum Einsatz. Für das Einbinden von menschlichen Aufgaben in Geschäftsabläufe (etwa für Eskalationsszenarien) stehen Human Workflows bereit. Dafür bietet 11g eine vorgefertigte Ajax-Worklist sowie umfangreiche Notifikationsmechanismen (SMS, E-Mail, Telefonanruf). Prozesse mit Massendurchsatz wiederum erfordern ESB-Techniken wie Datentransformation und Routing. Über Geschäftsregeln kann das Unternehmen das Programmverhalten auch nach dem Deployment anpassen, wenn es auf kurzfristig geänderte Rahmenbedingungen reagieren muss.

Erfahrungen aus EAI-Projekten mit Webservices zeigen, dass sich Qualität und Termintreue nur dann einhalten lassen, wenn die Webservices zuerst im Einzelbetrieb ihre Tauglichkeit bewiesen haben. Erst danach ist es sinnvoll, sie im Verbund zu begutachten. Ähnlich wie bei der objektorientierten Programmierung entscheidet auch bei der SOA-Entwicklung das begleitende Testen während der einzelnen Projektphasen über den Erfolg. Wer erst zum Entwicklungsende prüft, wird kein funktionstüchtiges Projekt abliefern. Aus diesem Grund hat Oracle das vom Vorgänger bekannte BPEL-Test-Framework für die Composites weiterentwickelt. Die Unit-Tests definiert der Programmierer im JDeveloper. Er kann sie sowohl interaktiv über die SOA-Konsole als auch im Batch mittels Ant ausführen.

Es war bisher notwendig, die zur Designzeit generierten WSDL-Dateien für die verschiedenen Test- und Produktionsumgebungen anzupassen. Unter Umständen sind diese Arbeiten ebenso aufwendig wie die eigentliche Entwicklung. 11g reagiert darauf mit den JSR-88-basierten Deployment Plans, die alle umgebungsspezifischen Konfigurationen enthalten und das von 10.1.3 bekannte Versionierungskonzept von BPEL-Prozessen auf die SOA Composites übertragen. Eine Composite wird mit dem SCA Packager in eine *.sar*-Datei mit einem *Revision Tag* gepackt, das die jeweiligen SCA-Komponenten enthält. Nach dem Deployment-Plan erstellt der EAR Packager aus weiteren JEE-Archiven wie *.war* oder *ejb.jar* das *.ear*. Letzteres lässt sich von JDeveloper, aus dem Fusion Enterprise Manager oder über die Kommandozeile mittels Ant auf dem Applikationsserver einrichten.

Weitere Neuerungen gibt es beim Monitoring und Management der SOA. Das Monitoring via BPEL- sowie ESB-Konsole ist jetzt in den Fusion Enterprise Manager integriert. Die Überwachung von Services erstreckt sich über alle involvierten Komponenten und gehört zur Enterprise Manager Fusion Middleware Control (EM FMC). Jede Prozessinstanz erhält eine ID, über die man suchen kann. Im Fehlerfall lässt sich die Instanz erneut ausführen und sogar als Unit Test speichern. Die zentrale Fusion-Komponente stellt der ESB, der mit über 200 Applikations- und B2B-Adaptern (SAP, CICS, EDI, RosettaNet et cetera) die Infrastruktur liefert. Er erledigt auch das Logging, Tracking und Monitoring für alle Services.

Um die Autorisierung, Authentifizierung und Nachrichtenintegrität für den Zugriff von außen kümmert sich der Policy Manager. Intern sind Service Component Interceptors für die Autorisierung bei jedem Übergang von einer Service-Komponente auf eine andere gemäß der Policies zuständig. Alle Sicherheitsprüfungen erfolgen zur Laufzeit. Hierzu verwendet der Policy Manager die standardisierte Java Platform Security.

Fazit

Wer sich die 3. Technology Preview des JDevelopers anschaut, bekommt eine klare Vorstellung davon, wie die elfte Generation der Fusion-Softwarepalette aussehen wird. Oracles neue Offenheit in Bezug auf Standards wird jedoch zum Preis einer niedrigeren Abstraktionsebene erkauft. Hier entsteht die Gefahr, dass die Entwickler sich in der Komplexitätsfalle verfangen und darunter ihre eigentliche Aufgabe – das Umsetzen von Geschäftsanforderungen – leidet. Mit der neuen Release sollte Oracle jedoch in der Lage sein, die Produkte aus den Aufkäufen der Firmen Siebel, Peoplesoft und JD Edwards in SOA-Applikationen zu fusionieren. (jd)

LARS NIEDERMEIER

ist unabhängiger Berater für Siebel CRM und EAI. Er setzt Oracles Fusion SOA Suite zusammen mit Siebel CRM zur Qualitätssicherung und Prozessoptimierung bei einer Schweizer Großbank ein.

Literatur

[1] Michael Stal; Standards; Am Anfang war SOA(P); Services und Komponenten mit SCA und SDO; *iX* 2/2007, S. 90







Webseiten prüfen mit Goolag

Tief graben

Michael Hamm

Ob Schwachstellen, verwundbare Webanwendungen oder versehentlich ins Netz gestellte sensible Daten – das Sicherheitswerkzeug Goolag hilft durch automatisierte Tests bei der Suche danach.

Innerhalb weniger Jahre entwickelte sich das sogenannte Google-Hacking – populär geworden durch die Recherchen von Johnny (I hack stuff) Long zu einer beeindruckenden Hacking-Disziplin [1]. Es war daher nur eine Frage der Zeit, bis jemand auf die Idee kam, diese Technik zu automatisieren und mit einer bequemen Benutzeroberfläche zu versehen. Seit Kurzem steht Interessierten für Sicherheitstests das unter der Affero GPL [2] verfügbare Werkzeug Goolag zur Verfügung, das nach Schwachstellen und verräterischen Informationen in Webauftritten sucht.

Es stammt von „Cult of the Dead Cow“ (cDc; www.cultdeadcow.com), einer Hackergruppe, die 1998 durch die Veröffentlichung des „Fernwartungswerkzeuges“ Back Orifice – das häufig missbräuchlich eingesetzt wurde – weltweite Berühmtheit erlangte. Und genau wie damals pocht heute ein Sprecher der Gruppe darauf, dass Goolag nicht als Hacker-Tool, sondern als Werkzeug zum Sensibilisieren der Verantwortlichen und Überprüfen der eigenen Sicherheit gedacht ist.

Goolag ist eine Windows-Anwendung, die man kostenlos auf der Webseite www.goolag.org herunterladen kann. Genauer gesagt, befinden sich im Download-Bereich Verweise zu den offiziellen Mirrors. Für Interessierte stellen die Anbieter ebenfalls die Sourcen bereit.

Starten, aber mit Gefühl

Nach dem Installieren blendet Goolag beim ersten Programmstart den „About“-Dialog als Willkommensnachricht ein. Der dort vorhandene Text „… popular search engines“ lässt vermuten, dass dieses Tool nicht nur Google, sondern auch alternative Suchmaschinen in seine Queries einbezieht.

Zurzeit ist das aber nicht der Fall. Beim Überwachen des Netzwerkverkehrs lassen sich lediglich Anfragen bei Google beobachten. Ein Blick in die mitgelieferte Google-Hack-Datenbank „gdorks.xml“ legt die Vermutung nahe, dass Goolag in dieser Version noch nicht fähig ist, andere Suchmaschinen anzusprechen.

Nicht alles, was geht, ist auch erlaubt

Weiter findet sich im Begrüßungsdialog ein Verweis auf Google’s Terms of Service, die Nutzungsbedingungen. Ihnen zufolge ist das, was das Werkzeug macht – das automatisierte Senden von Suchanfragen –, nicht erlaubt.

So ist beim ersten Experimentieren mit Goolag äußerste Vorsicht geboten, vor allem wenn man es von der eigenen Firma aus startet. Dann könnte Google schon nach wenigen Sekunden die lokale IP-Adresse sperren, was je nach Netzwerk-Topologie schnell zu Verstimmungen bei Kollegen, Managern und Systemadministratoren führen kann.

Die Bedienung des Werkzeugs ist intuitiv. Binnen weniger Minuten kann der Anwender den Funktionsumfang erfassen und verstehen. Das Hauptfenster (Abb. 1) unterteilt sich vertikal in zwei Bereiche. Linker Hand findet sich eine baumartig sortierte Liste der aktuell verfügbaren Google-Hacks, auch Google-Dorks genannt, zurzeit sind es 1418.

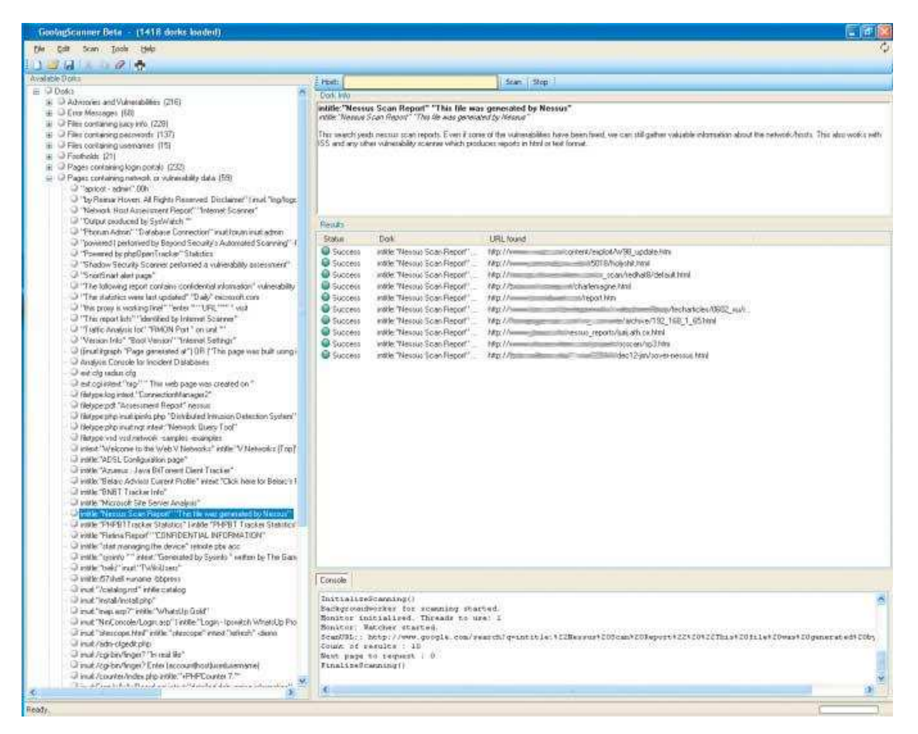
Die Google-Hacks sind je nach Thema in 14 Gruppen zusammengefasst, darunter Kategorien wie „Files Containing Passwords“, „Sensitive Directories“, „Vulnerable Servers“. Sowohl die Gruppierung als auch die Hacks selbst haben die Goolag-Programmierer offensichtlich 1:1 aus der Google Hacking Database von Johnny Long (johnny.ihackstuff.com/ghdb.php) übernommen. In ihr sind die Hacks nach dem Erscheinungsdatum sortiert, während Goolag sie alphabetisch auflistet.

Auf der rechten Seite der Anwendung befinden sich Informationen zum laufenden Scan. Dazu ist diese Bildschirmseite in die Bereiche „Dork Info“ „Results“ und „Console“ unterteilt. Der Erste zeigt den aktuell ausgeführten Google-Hack sowie Hintergrundinformationen an. Diese variieren von Hack zu Hack und beinhalten beispielsweise eine Beschreibung, den Namen des Autors oder gar Verweise zu existierenden Advisories und Exploits.

Im Results-Bereich erscheint eine Liste der bisher durchgeführten Google-Anfragen sowie deren Status und gegebenenfalls gefundene URLs. Der Status eines Google-Hacks kann sein:
– clean, in dem Fall hat Goolag keine verwundbaren Ziele gefunden;
– failed, was bedeutet, Google hat die Suchanfrage eventuell als Sicherheitsproblem erkannt und nicht beantwortet;
– success, Goolag hat Schwachstellen gefunden.

Im Eingabefeld „Host“ kann der Sicherheitstester einen zu überprüfenden Host- oder Domainnamen eintragen. Will er wahllos nach verwundbaren Zielen suchen, braucht er nichts einzutragen. Der eingetragene Host- oder Domainname wird unter der Haube in der Form *+site:foo.com* an den Google-Dork angefügt.

In der Praxis zeigt sich, dass ein kompletter Scan über alle 1418 Queries mindestens sechs Stunden dauern sollte. So kann man eine Blockade der eigenen



Bei Durchführung eines der links aufgeführten, thematisch gruppierten Hacks sieht der Sicherheitstester in der rechten Hälfte die Ergebnisse seines Scans sowie weitere Informationen (Abb. 1).

IP-Adresse bei Google vermeiden. Beim Setzen der entsprechenden Werte für die Scan-Geschwindigkeit in den Optionen ist also Zurückhaltung geboten.

Scan-Fortschritt plus die jeweiligen Ergebnisse kann man live in der Anwendung beobachten. Am Ende des Scans präsentiert ein kleines Popup-Fenster überdies eine kurze Zusammenfassung der Resultate.

Landet man einen Treffer (Success), und das Werkzeug hat eventuelle Schwachstellen gefunden, braucht der Anwender nur durch einfaches Anklicken der Zeile seinen Browser zu starten, der die entsprechende Webseite lädt. Nun kann man die Seite genauer untersuchen.

Wie bei allen Schwachstellen-Scannern ist es unerlässlich, alle Treffer manuell zu validieren, um die Fehlmeldungen – False Positives – zu eliminieren. Das ist zwar lästig, bei Weitem aber nicht so sicherheitskritisch wie False Negatives, also nicht identifizierte Schwachstellen.

Mehr Suchmaschinen gewünscht

Die Scan-Ergebnisse können leider in keiner Weise exportiert, ausgedruckt oder zu einem Report aufbereitet werden. Hier besteht noch reichlich Optimierungspotenzial für Weiterentwicklungen oder neue Anwendungen.

Auch beim Umgang mit den Google-Dorks sind Verbesserungen möglich. Wünschenswert wäre es auf jeden Fall, andere Suchmaschinen in die Abfragen einbeziehen zu können. Das ließe sich durch das Erstellen einer neuen Abstraktionsebene für eine suchmaschinenunabhängige Abfragesprache realisieren.

Eine Online-Update-Funktion für neu verfügbare Google-Dorks gibt es momentan nicht. Eigene Google-Hacks lassen sich zurzeit nicht über die Anwendung verwalten. Das bedeutet, man muss sie entweder via Texteditor in die Datei *gdorks.xml* oder gar in eine eigene Datei einpflegen.

Überdies wäre eine Funktion zum Verfeinern der gerade laufenden Suchanfragen eine sinnvolle Erweiterung. Von einem Werkzeug für ein umfangreiches Security Auditing ist Goolag noch ein ganzes Stück entfernt – allerdings war das vermutlich nicht die Intention der Entwickler.

Denen ging es offensichtlich viel mehr um ein gewisses Maß an Aufmerksamkeit und darum, für die Gefahren durch das stark unterschätzte Google-Hacking zu sensibilisieren. Zurzeit ist es einfach immer noch zu leicht, Zugangsdaten wie Passwörter, vertrauliche Informationen und verwundbare Webserver via einfacher Suchmaschinenanfragen zu finden. Hier bedarf es dringend der Aufklärung der Verantwortlichen.

Mit Goolag hat nun jeder die Möglichkeit, eigene Netzwerke zumindest auf die gröbsten Sicherheitsrisiken durch Google-Hacking zu untersuchen und sich gleichzeitig in die Materie einzuarbeiten. Womit Goolag genau das tut, was es soll: aufklären, sensibilisieren und eine erste Übersicht verschaffen.

Nach Aussagen von cDc (www.goolag.org/factsheet.txt) hatten die Gruppe sowie einige Testpartner Goolag intern bereits drei Jahre lang vor seiner Veröffentlichung eingesetzt – vorrangig um militärische und staatliche Netzwerke in den USA, Kanada, England, Frankreich, der Türkei und Saudi Arabien zu überprüfen. Angeblich entdeckten sie dabei so gravierende Lücken, dass sie die gefundenen Daten auch teilweise an das „Department of Homeland Security“ weitergaben.

Jedem Systemverantwortlichen kann man nur wärmstens empfehlen, das eigene Netzwerk mit Goolag auf offene Sicherheitslücken hin zu überprüfen – bevor es jemand anderes tut. (ur)

Daten und iX-Wertung

Goolag
Produkt: Sicherheitsscanner für Webseiten
Lizenz: Affero GPL
Betriebssystem: Windows

⊕ bedienungsfreundliches Werkzeug
⊕ zahlreiche, nach Themen gruppierte Hacks
⊕ sensibilisiert für Suchmaschinen-Hacks
⊖ keine alternativen Suchmaschinen
⊖ keine Export- oder Berichtsfunktion für Ergebnisse
⊖ keine Online-Update-Funktion

MICHAEL HAMM

ist Ingénieur Sécurité am Centre de Recherche Public Henri Tudor in Luxemburg.

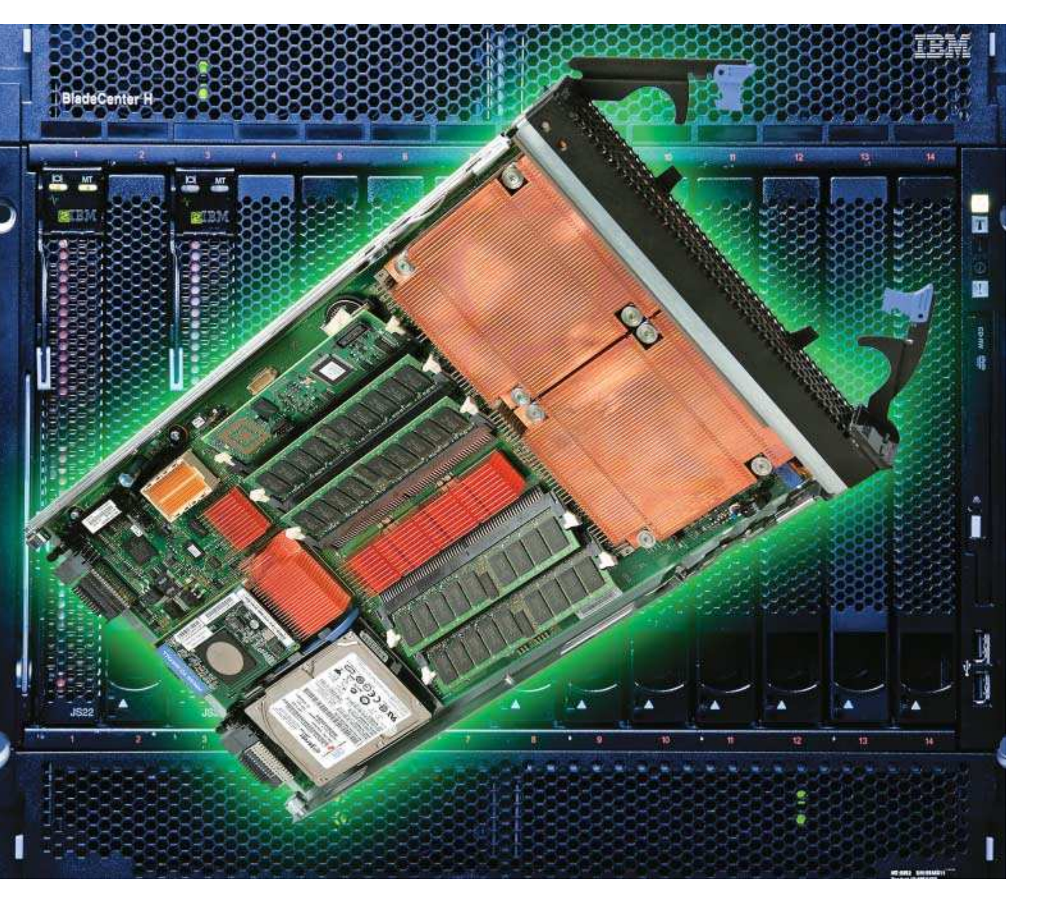
Literatur

[1] Michael Hamm; Netzsicherheit; Fein beobachtet; Suchmaschinen-Hacking: Was Google & Co verraten; *iX* 5/2006, S. 136

[2] Tobias Haar; Affero GPL Version 3; *iX* 2/2008, S. 26


iX-Link ix0806082





Bei der aktuellen Version sind es zwei, während Intel und AMD auf drei, vier und sechs aufgestockt haben. Im Gegensatz zu Intel hat IBM die Hardware-Thread-Technik beibehalten: pro Core zwei. Eine Power6-CPU mit zwei Kernen stellt dem Betriebssystem somit vier Recheneinheiten bereit.

Nach der Jungfernfahrt des Power6 in IBMs Midrange System i liefen beim System p die Blades vom Stapel. IBM bot zwei JS22 mit je zwei 4-GHZ-CPUs an. Sie verfügen wie die 4,7 GHz schnelle Variante über zwei Kerne pro Chip, denen je 4 MByte L2-Cache zur Verfügung stehen. Die eine Blade war mit AIX 6.1, die andere mit Suse Linux eingerichtet, und IBM hatte die hauseigenen XL-Compiler in der aktuellen Version (9.0) installiert. Beide Server waren mit 16 GByte Hauptspeicher voll bestückt, das Betriebssystem nebst der Entwicklungsumgebung befand sich auf lokalen Platten.

Start auf großer Plattform

Vom Systemvermieter Livingston kam das notwendige Kabinett. Aufbau und Start des Gesamtsystems nahm ein Techniker von IBM vor, anschließend ging es per DHCP ins Testnetz. Die üblichen Prozeduren waren flott erledigt, die Administration per Webbrowser im Out-of-Band-Netz bereitete keine Schwierigkeiten, abgesehen von den üblichen Geduldsproben, bis die Server die Interfaces für das Konsolen-Display hochgefahren hatten.

Von der Verarbeitung her gibt es nichts zu bemängeln. Die Blades sind servicefreundlich zu öffnen (wenn man es nicht auf der falschen Seite versucht) und gediegen – so gut wie keine Kunststoffteile. Die mit fast 5 kg nicht gerade leichten Server-Module gleiten sauber geführt durch Abdeckungen der inneren Luftschleusen in den Einbaurahmen und lassen sich leicht verriegeln. Das Umschalten auf KVM und Media-Laufwerk funktioniert weitgehend verzögerungsfrei. Nur wenn Keyboard samt Maus und Monitor am rückwärtigen Service-Modul angeschlossen sind, muss man unter Linux beim Fernzugriff über die Administrationssoftware auf die Konsole der Blade verzichten – etwas fürs Aufgabenheft bei Suse/Novell.

Im Laufe des Tests verlor die Blade mit Linux einen Teil ihres Hauptspei-

IBMs Power6 unter AIX 6.1 und Linux im Bladecenter

Zwei Sechser

Ralph Hülsenbusch

Fern von den umkämpften Grenzen der massenträchtigen Betriebssysteme und Prozessoren errichtet Big Blue eine Bastion für seinen RISC-Prozessor Power6 und sein Unix AIX 6. Allein der Schwenk von AIX 5L auf AIX 6 – ohne das Linux-L – spricht für sich.

Einen Paradigmenwechsel hat IBM auf Ebene 6 vollzogen: Die neue Power6-CPU – Power steht für „Performance optimized with enhanced RISC“ – steigert den Prozessortakt gegenüber dem Vorgänger Power5+ auf mehr als das Doppelte: 4,7 GHz statt bisher 2,2 GHz führen in eine neue Dimension. IBM steht noch beim 65-nm-Prozess wie Suns Ultrasparc T2 und Intels Itanium, beim Core 2 („Penryn“) ist Intel einen Schritt weiter mit 45 nm, AMD will noch 2008 mit Shanghai folgen. Aber mehr als 3,6 GHz sind dort bisher nicht zu sehen. Dafür versuchen die Chipschmieden, mit der Vervielfältigung der Kerne aufzuholen. Während es beim Power5 noch Module mit mehreren Prozessorchips waren – Multi Chip Modules (MCM) – besitzt der Power6 jetzt ebenfalls mehrere Kerne.

chers und erkannte nur noch 4 GByte. Versuche, Speichermodule zu tauschen, führten nicht weiter. Der Fehler musste im Memory-Controller stecken. IBM lieferte eine neue Blade, die sich selbst nach Hot Swap beim Allozieren des Speichers nicht irritieren ließ. Die Erklärung von IBMs Seite: *iX* habe die ersten Blades aus der Preproduction erhalten – die neue kam aus dem Produktionszyklus, aus dem die Kunden ihre Systeme bezögen.

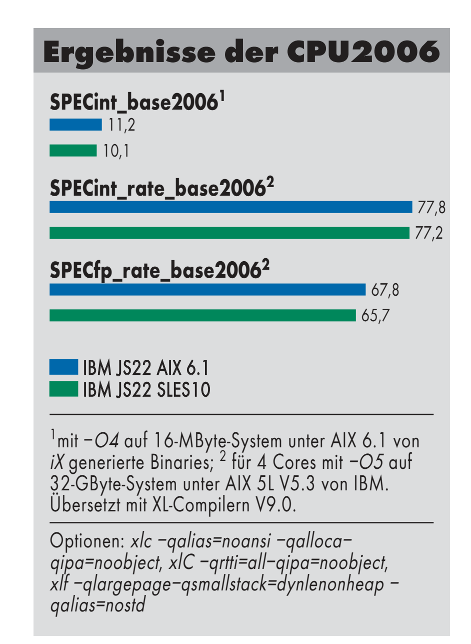
Für Optimierung zu wenig Speicher

Widerspenstiger verhielten sich beide Server beim Versuch, SPECs CPU2006 mit den XL-Compilern zu übersetzen. Dass Compiler bei 32 GByte Out of Memory laufen, scheint ein neuer Trend zu sein. Einen ähnlichen Effekt gab es bei Tests mit Suns Niagara [1]. Erst ein Verzicht auf Optimierung und *ipo* führt zu ausführbarem Code. Nur reichen die Benchmarks-Ergebnisse mit SPEC_int_base2006 von 11,2 (AIX) und 10,1 (Linux) bei Weitem nicht an die von IBM für die JS22 veröffentlichten heran. Erst eine Rückfrage in den USA beim Benchmarking förderte das zutage, was bei der SPEC sozusagen als Randbemerkung zu lesen ist: „The binaries were compiled on a system with 32 GB of memory.“ Man mag es kaum glauben, aber aus den USA kam die Bestätigung: „The larger memory is necessary in order for the compiler to perform its interprocedural analysis on some of the codes at high optimizations.“ – Das ist das härteste, was es bisher an Optimierung in der langen Geschichte des Benchmarking gab.

Auf dem Benchmark-Olymp

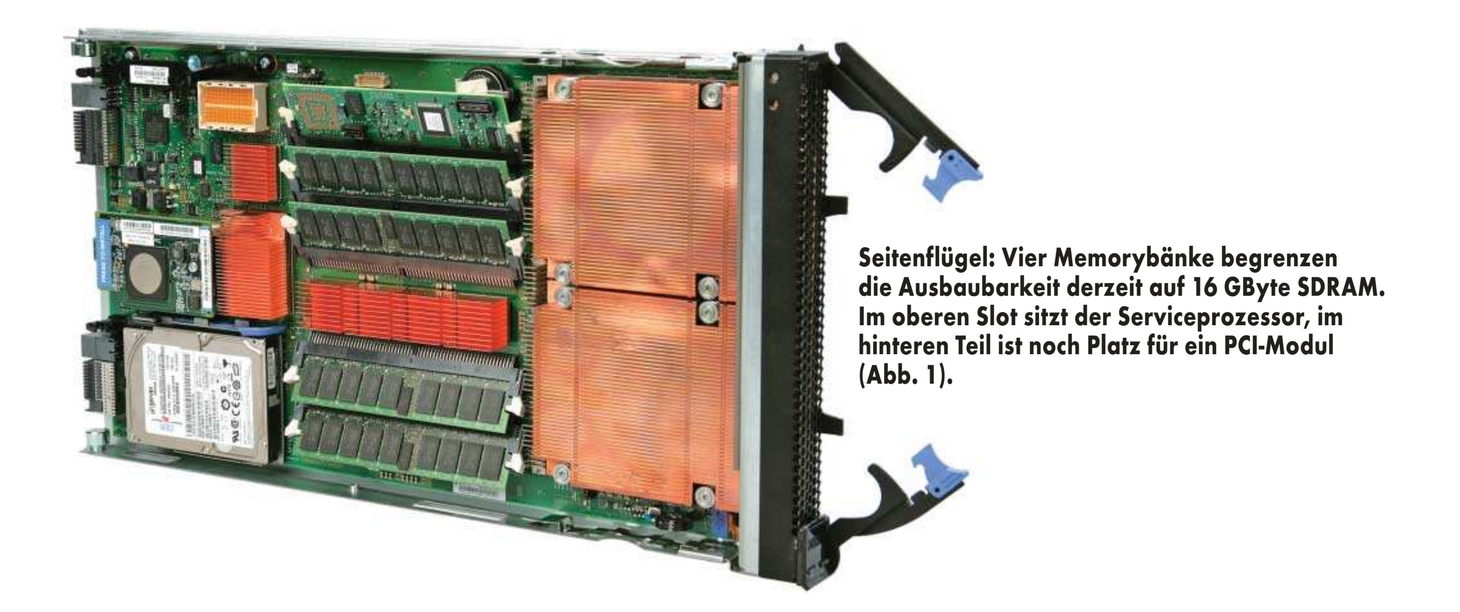
Da es nicht gelang, trotz mehrfacher Anfragen und Bemühungen bei IBMs Partnern an ein Power6-System mit 32 GByte heranzukommen, bleibt nur der Blick in die Tabellen bei der SPEC. Ausschlaggebend sind die Base-Werte, da sie aufgrund ähnlicher Bedingungen entstehen, wie sie bei der Programmentwicklung von kommerziellen Applikationen gelten. Peak-Werte gehören in die Klasse der olympischen Disziplin. Hier verwenden die Hersteller Optimierungen, die allenfalls jemand einsetzt, der seinen eigenen Sourcecode in- und auswendig kennt. Inzwischen zeigt die SPEC in ihrer Übersicht per Default nur noch Peaks. Man muss vorher auf „All SPEC CPU2006“ per „go“ umstellen.

Als Erstes fällt auf, dass Bull und IBM nur wenige Speed-Werte (Single Runs) veröffentlicht haben. Die J22 taucht erst bei Rate auf. Für ein System mit 4,7-GHz-Power6 erzielt IBM 17,8 unter AIX und 17,5 unter SLES10 SP1. In beiden Fällen verwendeten die Tester nur 32-Bit-Code und für AIX die ältere 5L-Version. Außerdem halfen



sie unter Linux mit der Smart-Heap-Library von Microquill nach, wie übrigens allen anderen Hersteller auch. Bricht man den SPECint_base2006-Wert auf 4,0 GHz herunter, kommt man für AIX auf 15,1, was immer noch zu weit weg von den wenig optimierten 11,2 liegt; Entsprechendes gilt für Linux.

Im Integer-Speed (SPECint_base 2006) muss sich der Power6 mit seinen 17,8 gegenüber einer X5460-CPU mit 3,16 GHz von Intel in einer Sun Fire geschlagen geben, die trumpft mit 24,3 auf. Ein deutlich anderes Bild entsteht beim Gleitkommarechnen:



Seitenflügel: Vier Memorybänke begrenzen die Ausbaubarkeit derzeit auf 16 GByte SDRAM. Im oberen Slot sitzt der Serviceprozessor, im hinteren Teil ist noch Platz für ein PCI-Modul (Abb. 1).

Hier tritt der Power6 im Speed-Run gegen eine 2,4 GHz schnelle SPARC64 VI mit 21,7 an und landet noch hinter Intels Core 2 Extrem (21,4) und Xeon (21,2) bei 18,7 SPECfp_base2006. Die Sparcs holen hier unter Solaris den Pokal, dichtauf sind Intels-CPUs unter Windows Vista64 Ulimate und SLES10.

Erreicht eine hohe Skalierung

Beim Multitasking kann der Power hingegen Bestzeiten einfahren. Mit acht Kopien auf vier Cores belegt er mit Abstand die ersten Plätze: 108 SPECint_rate und 102 SPECfp_rate. Verfolger Intels Xeon liegt mit 42,5 respektive 31,7 weit zurück. Doch die Sache hat einen Haken: Andere Prozessoren sucht man hier vergebens, denn acht Kopien auf vier Cores sind nur dann sinnvoll, wenn die CPU-Hardware Threads unterstützt. Intel hat aber bei seinen neuen Core-CPUs das Hyper Threading aufgegeben. Schaut man allein auf Messungen mit vier Kopien auf vier Cores, schließt Intels Xeon X5260 mit 70,1 und 51,0 etwas auf. Der Power6 skaliert mit 71 und 68 % (int und fp) deutlich besser als alle anderen Prozessoren. Mit 4,7 GHz gegenüber 3,3 beim Xeon läuft er aber erheblich hochtouriger. Unschlagbar ist der Power6 derzeit bei der Skalierung im SPECint_rate2006: Hier liegt er bei fast 100 %, selbst bei den Base-Resultaten.

Das heißt aber nicht, dass der Power6 erheblich mehr Energie verbraucht als die Gegenspieler: der Power6 liegt bei 100, der Xeon bei 120 und Suns UltraSparc T1 bei 180 Watt. Damit ist der Power6 nicht nur der Schnellste seiner Klasse, sondern auch der Energiesparendste. Noch ist er allerdings im Ranking der Systeme im SPECpower nicht zu finden.

Fazit

Mit dem Power6 hat IBM einen großen Schritt nach vorne geschafft. Allein die mehr als doppelt so hohe Taktrate gegenüber dem Vorläufer Power5+ bringt deutlich mehr Rechenleistung. Mit AIX 6 und den XL-Compilern können Entwickler Leistung aus dem Prozessor herauskitzeln, müssen dafür aber für den Hauptspeicher tief in die Tasche greifen. Außerdem brauchen sie ein solches System, um für kleinere, auf 16 GByte beschränkte Software entwickeln zu können. Zwar sind inzwischen die JS22 für 32 GByte deklariert, benötigen aber dafür 8-GByte-DDR2-SDRAM-Module – teuer und schwer zu beschaffen. Die jüngst vorgestellte JS12 mit ihren acht Memoryslots könnte einen Ausweg bieten, schlägt aber mit 3350 Euro zu Buche. Mit 32 GByte Hauptspeicher und zwei 73-GByte-Platten kommt man auf 9170 Euro.

Offensichtlich gibt es wegen der notwendigen großen und teueren Speichermodule derzeit Schwierigkeiten, an ein Power6-Systeme mit 32 GByte heranzukommen. Dass gute Optimierungen nur für wissenschaftliches Rechnen von Bedeutung sind, stimmt nicht ganz: Selbst bei den heute üblichen Einsatzbereichen von Blades als Server spielt schon allein das Ver- und Entschlüsseln eine wichtige Rolle, und dort geht es vor allem um Rechenleistung. (rh)

Literatur

[1] Ralph Hülsenbusch; UltraSparc; Der Niagara-Fall; Suns T5220 mit T2-Prozessor; *iX* 4/08, S. 104

[2] Andreas Leibl; Prozessoren; Round up; Neue Unix-Server von IBM mit Power5; *iX* 8/04, S. 103

Lieferumfang, Preise und iX-Wertung

JS22 Power6-Blade

Hardware: zwei Power6-CPU, zwei Kerne mit je zwei Hardware-Threads, 4,0 GHz, 4 MByte L2-Cache pro Core; 16 GByte ECC chipkill DDR2-SDRAM; 73 GByte SAS-Laufwerk, 2,5 Zoll; Netzverbindungen und Stromversorgung über Bladecenter H.; integrierter Systemmanagement Controller; Power Hypervisor

Software: AIX 6, SLES 10 (RHEL 4.6 zertifiziert); XL-Compiler 9.0

Hersteller: IBM (www.ibm.com)

Preis: 7620 Euro (Teststellung)

⊕ solide Verarbeitung

⊕ gute Skalierung der CPU

⊕ gutes Energie-Rechenleistungsverhältnis

⊖ hoher Speicherbedarf der Compiler

Fertiggeräte für den E-Mail-Verkehr

Vorbereitet

Bert Ungerer

Sowohl das Einrichten als auch das Betreiben von Mailservern gelten als komplex, fehlerträchtig und nicht zuletzt als rechtlich schwieriges Terrain. Davon profitieren Hersteller, die fertige Kombinationen aus Hard- und Software anbieten – inklusive Spam- und Virenfilter, denn ohne die geht praktisch nichts mehr.

Wer vor der Aufgabe steht, für seine Firma einen Mailserver (genauer „Mail Transfer Agent“, MTA) einzurichten, hat eine große Auswahl an Soft- und Hardware. Linux-Distributionen und Unix-Derivate enthalten Sendmail oder kompatible Mailserver wie Postfix oder Exim; solche wickeln bis heute einen Großteil des weltweiten E-Mail-Verkehrs ab. Darüber hinaus enthalten einige kommerzielle Bürosoftwarepakete, etwa Microsofts Exchange, IBMs Domino, Kerios Mailserver und andere Groupware eine MTA-Komponente.

Eine weitaus größere Auswahl besteht in Sachen Hardware, denn praktisch jeder aktuelle Desktop-PC oder ein vergleichbarer Rack-Server hat mehr als genug Leistungsreserven, mithilfe einer Mailserver-Software Hunderten von Anwendern das beliebte Internet-Medium zur Verfügung zu stellen.

Nach der Entscheidung für die geeignete Kombination aus Soft- und Hardware sowie deren Inbetriebnahme geht es ans Konfigurieren. Das bedeutet heutzutage vor allem, den Missbrauch des Sytems zu verhindern und die Anwender vor Unerbetenem zu schützen. E-Mail-Verantwortliche müssen sich zwangsläufig um das Ausfiltern von Datenmüll kümmern, denn über 90 Prozent aller E-Mails transportieren unerwünschte Werbung, Schadprogramme oder „vergiftete“ URLs. Auch unter kostenlosen und kommerziellen Spam- und Virenfiltern besteht eine reiche Auswahl. Eigentlich gibt es also mehr als genug Möglichkeiten für kompetente Postmaster, die Mail-Bedürfnisse ihrer Arbeitgeber zu erfüllen.

Pizzaschachteln im Serverschrank

Aber anscheinend gibt es zu wenige solcher Mail-Admins – oder sie sind zu teuer. Denn neben den selbst zu administrierenden Produkten hat sich ein ansehnlicher Markt für „schlüsselfertige“ Kombinationen aus Soft- und Hardware entwickelt. Für solche „Appliances“ – eine Bezeichnung, die simple Haushaltsgeräte einschließt – finden sich viele Käufer. Allein Barracuda Networks hat nach eigenen Angaben 50 000 Geräte bei Kunden aufgestellt.

Solche Appliances sind üblicherweise in 19-Zoll-Gehäusen untergebracht, die eine Höheneinheit, also gut



44 mm im Serverschrank belegen. Eine Ausnahme bildet der Business Server von Collax mit seinem Tower-Gehäuse (zu Komplett-Servern siehe auch S. 48 in dieser Ausgabe). Bei manchen Herstellern finden sich vom Kunden leicht zu ersetzende oder aufzurüstende Standardkomponenten, andere lassen nur den eigenen Service speziell „gebrandete“ Festplatten oder Speicherriegel ein- und umbauen. Bei solchen Geräten wird es entsprechend teurer, wenn sich herausstellt, dass die ursprünglich geplante Kapazität nicht ausreicht.

E-Mail bietet von sich aus Fehlertoleranz

In der Regel sind die Geräte mit zwei redundant angebundenen (RAID 1) Festplatten ausgestattet. Andere doppelt ausgelegte Baugruppen, etwa Netzteile, finden sich selten: So beliebt und wichtig E-Mail auch ist, erfordern gerade Mailserver relativ wenig Vorsorge gegen Ausfälle.

Auch wenn es Anwender gewohnt sind, E-Mails binnen Sekunden zu erhalten: Gerade dieses Medium stellt weder Echtzeit- noch Hochverfügbarkeitsanforderungen. Bei E-Mail handelt es sich ganz wie beim physischen Vorbild, der Papierpost, um ein „Store-and-Forward“-Medium. Es stellt lediglich sicher, dass auf dem Weg vom Absender zur Inbox des Empfängers keine Nachricht verloren geht, aber nicht, dass eine Mail innerhalb einer bestimmten Zeit ankommt.

Fällt eine Station vorübergehend aus, puffert der in der Zustellkette vorangehende Mailserver den Datenverkehr in einer Warteschlange und unternimmt mitunter einige Tage lang Zustellversuche (auch bei niedriger priorisierten Zielservern, falls vorhanden), bevor er es aufgibt und den Absender darüber informiert. Als das E-Mail-Protokoll SMTP vor 26 Jahren entstand, waren nicht einmal Standleitungen die Regel, geschweige denn Hochverfügbarkeit.

Die meisten Appliance-Hersteller statten ihre Rack-taugliche, doch PC-ähnliche Hardware mit Linux und dessen Mail-Komponenten aus. Beliebt sind Postfix für den Mailtransport und, falls die Appliance selbst E-Mails speichert, Cyrus als IMAP-Server. Einige Geräte arbeiten jedoch als reines Relay und setzen also einen separaten Mailbox-Server in der Firmeninfrastruktur voraus. Die Betriebssystembasis ist aus Leistungs- oder auch Sicherheitsgründen bei allen mehr oder weniger stark modifiziert, sodass offizielle Linux-Updates nicht zu gebrauchen sind. Für die in den Geräten arbeitenden Spezialdistributionen muss der Anwender darauf vertrauen, dass sicherheitskritische Updates schnell genug den Weg in das Fertiggerät finden.

Für die Spam- und Virenfilterung kommen neben den Open-Source-Produkten Spamassassin und ClamAV häufig proprietäre und entsprechend teurere Produkte zum Einsatz. Bei Godot und Sendmail findet sich zum Beispiel Elevens eXpurgate – ein Spam- und Virenfiltersystem, das Kunden, darunter große Provider, sonst als reine Dienstleistung in Anspruch nehmen.

Randbedingungen müssen erfüllt sein

Steht die Appliance erstmals im eigenen Serverraum unter Strom, geht es zunächst ans Konfigurieren. Vor der Anschaffung sollten sämtliche Details geklärt sein. Manche Kleinigkeiten können sich zu entscheidenden Hemmnissen auswachsen. So sollten sich etwa die IP-Adressen, Netzmasken und Default-Routen so einstellen lassen, dass sie zum eigenen LAN und Internet-Anschluss passen. Außerdem ist sicherzustellen, dass der bevorzugte Administrationsweg (etwa per SSH oder über einen eigenen Management-Anschluss) Unterstützung findet.

Nicht nur die Netzanschlüsse, auch der in der Appliance verpackte Mailserver will konfiguriert sein. Idealerweise sollte er nicht zustellbare E-Mails (Spam, Viren oder nicht existierende Empfänger) gar nicht erst annehmen. Damit entlastet er nicht nur sich selbst, sondern auch sämtliche nachgelagerten Systeme. Als entscheidenden Vorteil kann das Abweisen für sich verbuchen, dass im eigenen Netz keine „Bounces“ entstehen können, also etwa Benachrichtigungen über die Nichtzustellbarkeit an die Envelope-From-Adresse, die beliebig gefälscht sein kann. Die Verantwortung für die E-Mail bleibt durch das Abweisen (Reject) beim absendenden Mailhost.

Doch schon die Überprüfung, ob der vorgesehene Empfänger überhaupt existiert, scheint vielen Mailserver-Betreibern Schwierigkeiten zu bereiten. Die lästige Folge davon sind Bounce-Mails mit Unzustellbarkeitsbenachrichtigungen (Non-Delivery Report, NDN), die in alle Welt hinausgehen und im Falle von Spam und Viren allein (bis dahin) Unbeteiligte belästigen. Angesichts der Tatsache, dass der Anteil erwünschter Mails bei unter 10 Prozent liegt, sollten Admins sicherstellen, dass ihr Mailserver (ob in einer Appliance oder nicht) noch während des SMTP-Dialogs feststellt, ob ein Empfänger existiert, etwa per Abfrage eines Verzeichnisdienstes. Im Falle ungültiger Adressen sollte der MTA die Mail gar nicht erst annehmen.

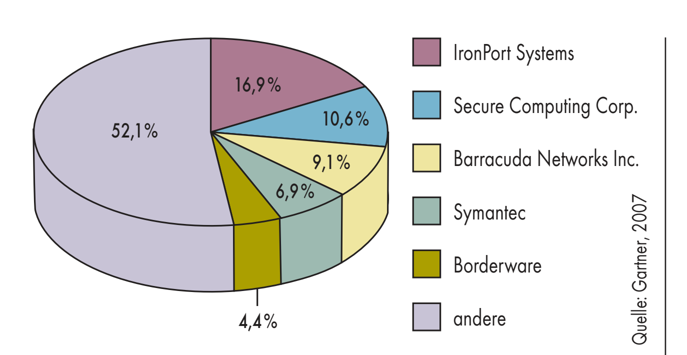
Ungeprüftes Annehmen schafft Verdruss

Ähnliches gilt für die Analyse der Mail-Inhalte. Doch viele Mailserver sind so konzipiert, dass sie E-Mails zunächst annehmen und dann erst auf Viren und Spam filtern. Laut Ironport besteht anderenfalls die Gefahr von Denial-of-Service-Angriffen, denn das Filtern dauert nun einmal eine gewisse Zeit. Immerhin teilte Ironport auf die Umfrage zu der vorliegenden Marktübersicht (siehe Tabelle am Ende des vorliegenden Artikels) von sich aus mit, dass das Einschalten von Bounces auf erkannte Spam- und Virenmails nicht empfehlenswert sei. Problembewusstsein auch bei Reddoxx: Der Her-

iX-TRACT

- Vorkonfigurierte Kombinationen aus Hard- und Software können E-Mail-Administratoren einen Teil der Konfigurations- und Wartungsarbeit abnehmen.
- Auf der PC-ähnlichen Hardware der Appliances läuft meistens ein Linux-Derivat, für dessen Wartung allein der Appliance-Hersteller verantwortlich ist.
- Auch eine „Fertiglösung“ entbindet Postmaster nicht davon, sinnvolle Einstellungen vorzunehmen, die den Verdruss über die Spam-Plage nicht nur bei regulären Anwendern, sondern auch bei Unbeteiligten in Grenzen halten.

Im umkämpften Markt für kombinierte E-Mail-Hard- und Software verkaufen sich Ironport-Appliances derzeit besonders gut (Abb. 1).



steller teilte mit, dass sich bei der Appliance SpamFinder die Bounces abschalten lassen, ohne dass explizit danach gefragt worden war.

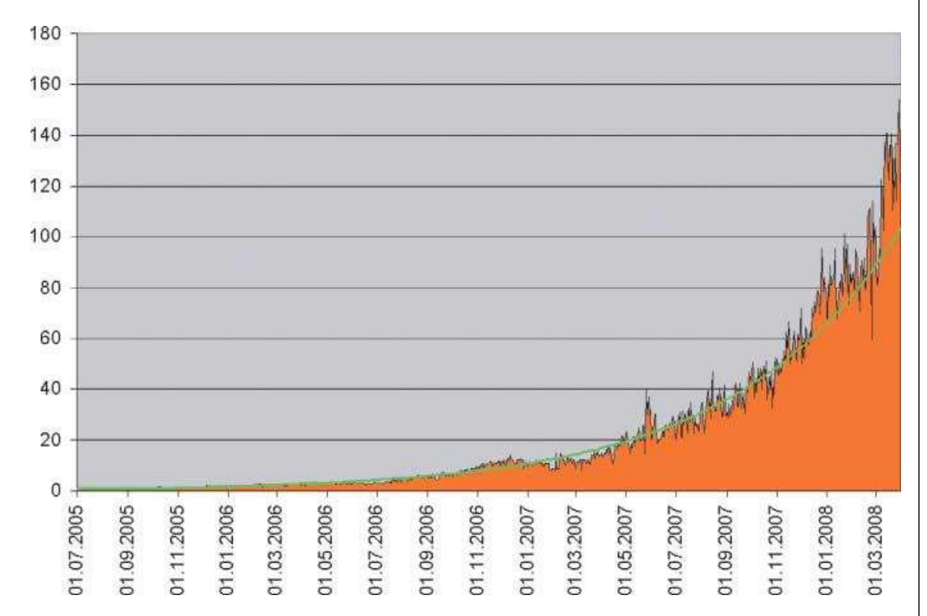
Auch Barracuda Networks setzt auf das Annehmen vor dem Filtern, mit der Begründung, dass die SMTP-Sitzung so schnell wie möglich beendet sein sollte. Doch während Ironport davon abrät, bei erkannten Spam- und Virenmails Bounces zu generieren, sieht sich Barracuda durch die RFCs dazu verpflichtet, die Grundeinstellung seiner Appliances so zu wählen – neben der großen Verbreitung der Geräte ein Grund dafür, dass viele eigentlich Unbeteiligte laufend E-Mails mit Betreffzeilen wie „Message you sent blocked by our bulk email filter“ erhalten, denn Spam- und Virenmails tragen selten authentische Absenderadressen.

Dass man unerwünschte Mails aber auch abweisen kann, statt Bounces in alle Welt zu versenden, zeigt unter anderem die Sponts-Appliance von der iKu AG.

So verlockend die Angebote der Appliance-Hersteller sind, ein Grundverständnis für das eigene Unternehmensnetz und das Medium E-Mail setzen auch sie voraus. Hier sind die Beratung seitens der Hersteller und die Grundeinstellungen der Geräte entscheidend. Spam- und Virenmails mit automatisch erzeugten Bounce-Mails zu beantworten, sollte heutzutage nicht mehr zu den Grundeinstellungen gehören.

Fazit und Ausblick

Noch ist der Markt für Mailserver- und -Filter-Fertiggeräte vielfältig. Eine Konsolidierung findet jedoch bereits statt und hat ihren vorläufigen Höhepunkt mit dem Kauf von Ironport durch Cisco im vergangenen Jahr erreicht. Kaum dass diese Übernahme abgeschlossen war, gab es an anderer Stelle einen Paukenschlag: Google erwarb den E-Mail-Dienstleister Postini. Die Musik spielt mittlerweile auch dort, wo die Unternehmen selbst gar nichts mehr mit eigenen Mailservern zu tun haben wollen, sondern den Dienst komplett zu Anbietern wie



Laut dem Mailfilter-Dienstleister Eleven, der diese erschreckende Statistik erstellt hat, ist ein Ende der Spam-Flut nicht in Sicht. Eine Einschätzung, die leider den Erfahrungen vieler E-Mail-Anwender entspricht (Abb. 2).

E-Mail-Appliances für den Unternehmenseinsatz

Hersteller oder Marke	Barracuda Networks	Clearswift GmbH	Collax GmbH	CP Secure GmbH	godot GmbH	iKu AG
Web	www.barracuda.com	www.clearswift.de	www.collax.com	www.cpsecure.de	www.godot.de	www.sponts.de
E-Mail	obareiss@barracuda.com	info@clearswift.de	info@collax.com	info@cpsecure.de	vertrieb@godot.de	sponts@iku-ag.de
Produkt (Beispiel für 200 Anwender)	Spam Firewall 300	MIMEsweeper	Collax Business Server >> Office Power	CSG-110	go.mail Security Gateway	Sponts/Complete
Hardware	1 HE, 1 Ethernet-Anschluss (10/100)	Dell-Hardware, virtualisiert auf eigener Hardware oder für VMware ESX Server	Tower-Gehäuse, Intel E6420, 2 GByte RAM, 2 × 160 GByte HD, 2 × LAN (GE)	1 HE, P4 Celeron 2 GHz, 512 MByte RAM, 40 GByte HD, 3 × LAN 10/100	1 HE, Opteron 1210, 4 GByte RAM, 2 × 250 GByte HD, 2 GE-Anschlüsse	1 HE, Intel Core 2 Duo E4500, 2,2 GHz, 1 GByte RAM, 2 × 250 GByte HD
Aufrüstung durch Kunden möglich	–	✓	✓	–	✓	✓
Betriebssystem/ Mailsoftware	Open Source	Linux, Sendmail	Linux mit 2.6er-Kernel, Postfix, Cyrus	Linux	go.OS, Postfix, Cyrus	Linux mit 2.6er-Kernel, Sponts
E-Mail-Funktionen						
externe Blacklists einbindbar	✓	✓	✓	✓	–	✓
Spam-Filter	✓	eigener	Spamassassin	Commtouch (optional), eigene Heuristik	eXpurgate	eigene Heuristik
AV-Engine	✓	Kaspersky	Kaspersky, Antivir	Kaspersky, CP Secure	Avira Antivir	Avira, Kaspersky, Sophos, ClamAV
Rejects nach Filterung	–	✓	–	✓	✓	✓
weitere Mechanismen der Spam- und Viren–behandlung	Markieren, Quarantäne	Markieren, Quarantäne	Markieren, Quarantäne, Verwerfen, Bearbeitungs-Queue	Markieren, Quarantäne	Markieren, Quarantäne (Public IMAP Folder), Umleiten	Markieren, Zustellen trotz Reject, fallweise Greylisting, Teergrubing
Bounces auf erkannte Spam-/Virenmails	✓ (abschaltbar)	✓	–	–	✓	–
Empfängerverifizierung	LDAP, SMTP	LDAP, ADS, Domino, statische Liste	LDAP	–	LDAP, ADS	SMTP, statische Liste
Filterregeln durch Anwender	✓	–	✓	–	–	✓
Anwender-Filterregeln durch Administrator	✓	✓	–	–	–	✓
Postfachserver integriert	–	–	✓	–	✓	✓
Systemmanagement						
SSH übers LAN/Internet	–/✓ (nur durch den Service)	✓/✓ (IP-Adressen festlegbar)	✓/✓	–/✓ (SSL/nur Service)	✓/✓ (Service; Kunden eingeschränkt)	✓/✓
separater Management-Anschluss	–	wahlweise einer der LAN-Ports	✓	✓	–	✓
Hersteller kann auf E-Mail-Verkehr oder -Inhalte schließen	–	–	–	–	–	–
Reporting für Admins	Web, E-Mail	Web, div. Exportformate	Web, PDF	Web, TXT, CSV	Web, E-Mail, Logdateien	Web, E-Mail, CSV
Anwenderschnittstellen	E-Mail-Reports, Outlook-Plug-in, Web	je nach Rollendefinition	Web, Webmailer	Web, E-Mail	Web	Web, E-Mail
Preisbeispiel (200 Anwender)	2399 Euro + jährlich 499 Euro	4600 Euro + jährlich 2100 Euro	3260 Euro + jährlich 2345 Euro	2990 Euro + jährlich 897 Euro (ab 2. Jahr)	8500 Euro + jährlich 6000 Euro (ab 2. Jahr)	4260 Euro + jährlich 1090 Euro
Besonderheiten, Extras	automatisierte Backups, halbstündliche Updates, Echtzeit-Virenschutz, Verschlüsselung	zeitgesteuertes Backup, zentrales Management mehrerer Appliances, automatisierte Updates	Unified Messaging, Backup/Restore, reine Softwareversion erhältlich	transparentes Scannen (kein MTA); Commtouch (15 % Aufpreis)	Virenausbruchserkennung, Webmailer und Firewall	Online-Restore über Web-Interface, SQL-Interface, Active-Active-Cluster-fähig

✓ = vorhanden, – = nicht vorhanden, k. A. = keine Angabe

Messagelabs, Antispameurope, Eleven oder eben Postini auslagern. Angesichts der Tücken, die das Mailgeschäft birgt, ein sicherlich attraktives und zukunftsfähiges Geschäft. (un)

Literatur

[1] Lukas Grunwald, Bert Ungerer; Nachrichtensperre; Borderwares Mail-Firewall MXtreme; *iX* 7/2004, S. 56

[2] Lukas Grunwald, Bert Ungerer; Mailmaschine; Ironports Messaging Gateway Appliance C60; *iX* 10/2004, S. 78

[3] Lukas Grunwald; Abweisend; Antispam-Appliance für den Mittelstand; *iX* 12/2004, S. 60 (über Sponts von iKu)

[4] Lukas Grunwald; Lautpost; Antispam-Appliance von 3Com auf Borderware-Basis; *iX* 7/2005, S. 84

[5] Andreas Erbe, Christian Schommer; Tunnelstation; Antispam-Appliance auf Open-Source-Basis; *iX* 1/2006; S. 96 (über Barracudas Spam Firewall 600)

[6] Bert Ungerer; Eingeschränkt; IP-Blacklists gegen unerwünschten Datenverkehr; *iX* 4/2007; S. 102

[7] Christoph Puppe; Leidtragende; Spam aussortieren als Dienstleistung; *iX* 8/2007, S. 72 (Eleven vs. Antispameurope)

Intra2net AG	IronPort Systems	Reddoxx GmbH	Sendmail GmbH	Sonicwall	Sophos	Telco Tech GmbH	underground_8 gmbh
www.intra2net.com	www.ironport.de	www.reddoxx.de	www.sendmail.com	www.sonicwall.com	www.sophos.de	www.telco-tech.de	www.underground8.com
info@intra2net.com	de-info@ironport.com	sales@reddoxx.com	germany@sendmail.com	germany@sonicwall.com	info@sophos.de	info@telco-tech.de	office@underground8.com
Intranator Appliance Pro 250+	C150	SMB	Sentrion MP 301	Email Security 300	ES1000	LiSS 3000+ Filter-Modul	Limes AS 500
1 HE, Intel Xeon 3075, 4 GByte RAM, 2 × 500 GByte HD, 3 × LAN (GE)	1 HE, Intel, 2 × 80 GByte HD, 2 × LAN (GE)	1 HE, 3,0 GHz, 512 MByte RAM, 2 × 75 GByte HD, 2 × LAN (GE)	1 HE, Intel Dual Core, 8 GByte RAM, 2 × 146 GByte HD (15.000/min), 5 × LAN, redundante Stromversorgung	1 HE, 2,66 GHz, 1 GByte RAM, 80 GByte HD	Celeron D 2,53 GHz, 1 GByte RAM, 160 GByte HD, 2 × LAN (GE)	1 HE, 2,4 GHz Core 2 Duo, 512 MByte RAM, 80 GByte HD, 6 × LAN (GE)	1 HE, Intel Celeron 2 GHz, 1 GByte RAM, 80 GByte HD, 4 × LAN (10/100)
✓	–	–	–	–	–	✓	–
Intranator Linux (2.6er), Postfix, Cyrus	AsyncOS	Linux mit 2.4er-Kernel	Sentrion MPE 3.1	k. A.	FreeBSD-Variante, Postfix	Linux mit 2.6er-Kernel, qmail	Ubuntu-Variante, Postfix
✓	–	✓	✓	✓	eigene	✓	✓
Spamassassin	eigener	eigener	Cloudmark, Commtouch, eXpurgate	eigener	eigener	eigener (Saucer)	Spamassassin/eigener
F-Secure integriert	McAfee, Sophos, Virus Outbreak	ClamAV	McAfee	Kaspersky, McAfee	eigene	Avira, ClamAV	ClamAV, Kaspersky
–	–	✓	✓	✓	–	✓	–
Markieren, Quarantäne, Umleiten	Quarantäne, Traffic-Begrenzung	Markieren, Quarantäne	Markieren, Quarantäne, Traffic-Begrenzung	Markieren, Quarantäne, Umleiten, Bounces, Traffic-Begrenzung, Verwerfen	Markieren, Quarantäne	Markieren, Quarantäne	Markieren, Quarantäne
–	✓ (nicht empfohlen)	✓ (abschaltbar)	✓	✓	✓	✓	✓
LDAP, ADS, SMTP	LDAP, ADS, NDS, Lotus Notes etc.	ADS, Domino, OpenLDAP	✓	LDAP, ADS, Domino etc.	alle LDAP-basierenden, SMTP	ADS, LDAP, eDirectory	– (LDAP, ADS angekündigt)
✓	–	–	✓	✓	–	–	–
✓	✓	✓	✓	✓	✓	–	✓
✓	–	–	✓	–	–	–	–
✓/✓ (Service, wenn autorisiert; Kunde optional)	✓/✓ (falls vom Kunden gewünscht)	✓/✓	✓/✓ (nur vom Service)	–/–	–/✓ (nur Service, auf Kundenwunsch)	–	–
–	✓	–	Dell Remote Access Controller	–	✓	wahlweise einer der LAN-Ports	–
–	Statistiken, falls vom Kunden gewünscht	–	–	nur Statistik	✓ (auf Kundenwunsch)	–	–
Web, E-Mail	Web, E-Mail (PDF), SSH, SNMP	Windows-GUI	Web	GUI, E-Mail (PDF)	Web, Exportfunktion	Web, E-Mail	Web, E-Mail
Web, E-Mail	Web, E-Mail	Windows-GUI, E-Mail, Plug-in für Outlook ab 2000	Web, E-Mail	Web, E-Mail	Web, E-Mail	Web	– (Quarantäne-Zugriff angekündigt)
6790 + jährlich 1250 Euro ab 2. Jahr	3750 Euro + jährlich ab 1650 Euro (ab 2. Jahr)	2990 Euro + jährlich 790 Euro	auf Anfrage	2795 USD + jährlich 640 USD	auf Anfrage	4000 Euro, keine laufenden Kosten	2290 Euro + optional jährlich 499 – 838 Euro
Webmailer, 12 Monate Updates inkl.	E-Mail-Verschlüsselung	Challenge-Response-Verfahren, VMware-Version; Verschlüsselung und Archivierung optional	S/MIME, RPost, IM	statistische Analysen für „Time Zero Protection“	„Proactive Monitoring“ enthalten	Option: Cobion-URL-Filterung, Firewall, IPS, VPN	Greylisting



Besonderheiten von Industrie-PCs

Auf Montage

Axel Urbanski

Ein Blick über den Zaun in Richtung x86 Industrie-PC lohnt sich, denn dort gibt es Altbekanntes und Neues zu entdecken. Solche Systeme müssen ihre Dienste oft in belasteter Umgebung verrichten, was besondere Forderungen an sie stellt.

Industrie PCs (IPCs) haben ihren eigenen Markt, in dem spezielle Spielregeln gelten. Er teilt sich in drei Hauptbereiche ein:
– Single Board Computer,
– Systeme mit ITX/ATX-Mainboards und
– Rechner, die Backplanes nutzen.

Zu den Gemeinsamkeiten zählt vor allem die Verwendung von Chips für den Embedded-Markt. Intel ist bei den CPUs und Chipsets Marktführer. Der Grund liegt in den langen Liefergarantien für die Komponenten, wie sie in dem Marktsegment gefordert sind. Während der Embedded World 2008 hatte Intel den Verfügbarkeitszeitraum auf sieben Jahre erhöht. VIA spielt mit seinen C3- und C7-CPUs nebst passenden Chipsätzen mit und garantiert wie AMD für seine Prozessoren fünf Jahre, Hersteller kompletter Systeme können daher ähnliche Zusagen für die Lieferbarkeit geben und ihre Produkte deutlich länger am Markt halten als bei herkömmlichen PCs üblich.

Technische Neuerungen mit Bedacht

Ohne Weiteres kann man heute noch Mainboards für den Pentium III (PIII) mit dem in der PC-Szene einst beliebten BX-Chipset und passenden CPUs bekommen. Neben den VGA- und DVI-Anschlüssen gibt es eine direkte Ansteuerung von LCD-Panels auf vielen Boards. Ältere verwenden einen TTL-Anschluss (24 Bit), neuere liefern die Grafik via LVDS (Low Voltage Differential Signaling) an das Display. Hierfür greifen die Hersteller auf die im Chipset integrierten oder einfache Module zurück, wie sie bei Servern üblich sind.

Die Mehrheit der Boards besitzt einen Steckplatz für Flash-Speicher, entweder als DOC (Disk on Chip) von M-Systems oder in Form von CF-Adaptern (Compact Flash). Passende CF-Karten stellen eine Alternative zu Festplatten dar und sind deshalb über den Sockel an den IDE-Bus angeschlossen. Die DOCs dienen ebenfalls als Festplattenersatz, der 32-polige DIL-Sockel (Dual In-line Package) benutzt allerdings nicht den IDE-Bus, sondern greift auf ISA/PCI-Bus zu. Die Technik blendet den Flash-Speicher in einem 8 KByte großen Fenster in den Hauptspeicher ein. Sowohl Linux als auch Windows 2000 und XP können mit den DOCs umgehen; derzeit sind 16 bis 1024 MByte große Module am Markt.

Der Sicherheit dient ein integrierter Watchdog. Im Kern besteht ein solcher Wachhund aus einem Zähler, der, einmal angestoßen, rückwärts läuft. Erreicht er die Null, löst er einen NMI (nicht-maskierbaren Interrupt) aus und startet den Rechner neu. Die zu überwachende Software setzt im normalen Betrieb den Zähler regelmäßig vor dem Ablauf wieder auf den Anfangswert. Stürzt sie ab, springt der Zähler nicht zurück, der Watchdog schlägt zu und startet den Rechner neu.

Es gibt nur wenig Einschränkungen bei der Auswahl des Betriebssystems. Sofern Treiber für die Komponenten vorhanden sind, geht alles von DOS bis zu Windows Server über Linux, BSD oder Solaris bis hin zu Echtzeitbetriebssystemen. Die Chiphersteller setzen auf eine kleine Auswahl qualifizierter Chipsets und CPUs. Es gibt wenig Neuentwicklungen, sondern in der Regel Anpassungen. Gleiches gilt für die speziellen CPUs. Im Vordergrund steht ein niedriger Energieverbrauch, denn in Industrieanlagen ist es schwierig, für Kühlung zu sorgen. Ein sparsamer lüfterloser PC passt gut in ein rundum geschlossenes Gehäuse, das gegen Staub und Nässe geschützt ist.

Kleiner geht doch

Ein gutes Beispiel für die Miniaturisierung von IPCs ist der Mops PM von Kontron. Auf nur 90 × 96 mm²

befindet sich ein kompletter Pentium-M-Rechner mit bis zu 1,4 GHz [a]. Neben einer parallelen, zwei seriellen Schnittstellen, zwei für USB 2.0, je einer für EIDE und CF sowie einer LAN- und VGA-Schnittstelle existiert noch eine weitere für LVDS-Grafik. Das Modul ist über einen PC104Plus-Bus [b] erweiterbar. Dahinter verbirgt sich der alte ISA-Bus, der auf zwei zweireihige Pfostenreihen gelegt ist. Der lange zweimal 32-polige Pfostenverbinder ist an den 8-Bit-Teil des ISA Busses gekoppelt, der kurze, zweimal 20-polige an die 16-Bit-Erweiterung. Sowohl Platinengröße als auch Lage der Stecker sind spezifiziert. Da noch ein PCI-Bus hinzukommt, nennt sich das Ganze PC104Plus. Er endet in einem vierreihigen, 120-poligen Steckplatz. Die passenden Module kann man einfach ineinanderstecken und stapeln. Auf der Unterseite der Platine ragen die Stiftleiten heraus, oben befinden sich die passenden Buchsen.



MOPSig: Auf dem kleinen Komplettrechner im PC104-Format verbergen sich die Anschlüsse für PCI, USB und CRT in der weißen Steckleiste. Vorne sind die ISA-Steckplätze zu erkennen, der Hauptspeicher sitzt auf der Unterseite (Abb. 1).

115 × 165 mm^2 belegt ein Single Board Computer (SBC) im EPIC-Format (Embedded Platform for Industrial Computing) an Fläche und mit 146 × 203 mm^2 schlägt das EBX-Format (Embedded Board eXpandable) zu Buche. Da ein EPIC-Board nicht viel größer als ein Stück Kuchen ist, tauchen die SBCs bis zu dieser Größe unter der Rubrik „Biscuit-PC“ im Handel auf. Als Nächstes wollen die Entwickler zusätzlich PCI-Express integrieren, was zu der Bezeichnung PC104-Express führen wird. Geplant sind ein 4x- und ein 16x-PCIe-Anschluss auf dem kleinen Format von 90 × 96 mm^2. Module für das Format sind derzeit auf dem Markt rar.

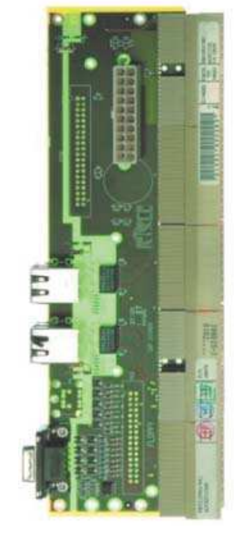
Verwandtschaft zum Normal-PC

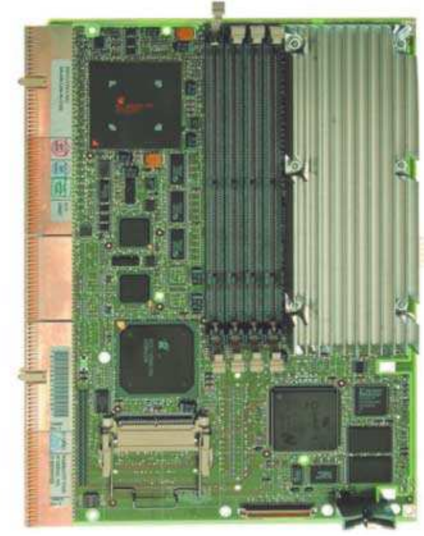
Bei den ATX-, microATX- und ITX-Mainboards ist die Nähe zu den bei PCs üblichen Boards unverkennbar. Bei IPCs sind die Chipsets in erster Linie für Strom sparende CPUs ausgelegt. Viele der Boards erlauben den Anschluss von LDVS-Panels oder die Verwendung von CF-Karten. Für manchen Einsatz eignen sich vor allem die P4-Boards mit ISA-Steckplätzen, denn häufig sind Steuer- und Messkarten, die diesen Bus nutzen, hochpreisig oder nur schwer zu ersetzen. Außerdem können Ingenieure Eigenentwicklungen auf der Basis von ISA recht einfach realisieren. Eine wichtige Gruppe von IPCs bilden die Systeme mit eigener Backplane, die alle Komponenten miteinander verbindet. Der eigentliche Rechner besteht aus einer Einsteckkarte, was die Wartung der Systeme vereinfacht. Ordnung in die Anschlüsse bringt die Einteilung nach PICMG-Spezifikationen der PCI Industrial Computer Manufacturers Group [c], die circa 450 Mitglieder hat.

Die jüngste der PICMG-Spezifikationen trägt die Nummer 3, besser bekannt als Advanced Telecommunications Computing Architecture oder AdvancedTCA (ATCA) [e]. Die Spezifikation entstand ursprünglich für Telekommunikationsanwendungen.

Die 19-Zoll-Racks müssen nur 60 cm tief sein, die senkrecht eingebaute Platine ist 8 Baueinheiten hoch und 280 mm tief. Vorne sind die Anschlüsse für optische, hinten die für Kupferkabel. Weder Hotplugging noch die Begrenzung der Leistungsaufnahme auf 200W je Board hat die PICMG vergessen. ATAC beschränkt sich nicht auf x86-Server, es gibt Boards mit Signalprozessoren und PowerPCs oder Suns Sparcs [f]. Sechs Unterspezifikationen definieren Ethernet, Infiniband, StarFabric, PCI-Express, RapidIO und PRS.

Bei PRS handelt es sich um Packet Routing Switches, RapidIO bezeichnet ein paketorientiertes, bis zu 60 GBit/s schnelles, geschaltetes (über Switch gekoppeltes) Verbindungsverfahren, das vom Durchsatz her zwischen PCI-Express und Ethernet liegt. StarFabric erlaubt es, PCI-Systeme zu erweitern und definiert Methoden, diese zu verbinden. Beim Aufbau von Clustern kann man StarFabric durchaus in Erwägung ziehen. Für einige Anwendungen war ATCA zu groß, deshalb entstand zusätzlich microTCA mit 3 bis 6 U (Baueinheiten im Rack) Höhe und 181 mm Tiefe der Platine. Diese Entwicklung





Doppeleuro: Rechts das cPCI-Mainboard mit Speicher und CPUs, links die I/O-Steckkarte, die entweder direkt oder auf die Backplane aufgesteckt wird (Abb. 2).



Senkrechtstarter: Das ATCA-Board steckt senkrecht im 8 U hohen Gehäuse, hier eine Multiprozessor-Blade, die Anschlüsse an die Backplane sind oben im Bild zu erkennen (Abb. 3).

ist recht originell, da einer der Hauptgründe für die Schaffung des Standards war, dass CompactPCI-Platinen für ATCA zu klein sind.

Die Spezifikation für CompactPCI (cPCI) findet sich unter PICMG 2.xx wieder. Dessen Platinengröße ist auf das Eurokartenformat (100 × 160 mm^2) oder Doppeleurokartenformat (233 × 160 mm^2) beschränkt. Es sind acht Karteneinschübe vorgesehen. cPCI-Rechner findet man häufig in der Mess- und Regeltechnik. Die Zahl von 20 Unterspezifikationen zeigt, wie weit das Einsatzgebiet ist. Von besonderer Bedeutung sind die Hotswap-Technik und die Redundanz der Systemslots, weil das die Möglichkeit eröffnet, das CPU-Board im laufenden Betrieb zu tauschen. Die Nutzung des cPCI-Formates beschränkt sich ebenfalls nicht auf x86-Rechner.

PICMG 1.x betrifft nur x86-IPCs. Auf der Backplane befinden sich normale Steckplätze zur Erweiterung. Je nach Bauform passen ISA-, PCI-, PCI-X- oder PCI-Express-Karten. Der eigentliche Rechner sitzt auf einer Slotkarte, die einer vollformatigen PCI-Karte entspricht. Im Grundstandard von PICMG 1.0 ist mindestens ein Steckplatz dafür vorgesehen. Es sind bis zu vier 32-Bit-PCI-Steckplätze definiert, die der Hersteller um weitere für ISA ergänzen kann. Über insgesamt 20 Slots verfügen die größten Backplanes, wobei zwei für die CPU-Karte vorgesehen sind. Maximal stehen also bis zu 14 ISA-Slots zur Verfügung, was dazu führt, dass die CPU-Karten immer noch Treiber für den ISA-Bus enthalten.

Alter Bus in voller Fahrt

Aber ISA gehört nicht mehr zu den aktuellen Bussen. Daher enthält die Definition 1.1 PCI-PCI-Bridges, um die Zahl der PCI-Steckplätze zu erhöhen, allerdings auf Kosten der passiven Backplane. Beliebt als PCI-PCI-Bridge sind Intels 21152-Chips, die man oft auf Mehrfachnetzwerkkarten findet. Der Chip macht aus einem PCI-Steckplatz vier. Es sind durchaus Backplanes mit 12 solcher Slots erhältlich. Geht es um PCI-X, kommt die 64-Bit-Version der PICMG infrage. Zwar ist PICMG 1.2 moderner, dort fehlen aber die ISA-Slots. Soll PCI-Express hinzukommen, empfiehlt es sich, auf den Standard PICMG 1.3 zu setzen.

Zwei Bussysteme im engen Verbund

Wenn die PICMG-Slot-Karten für die CPU zu groß sind, bietet sich PCISA an. Die Bezeichnung ist eine Zusammensetzung aus PCI und ISA. Gegenüber PICMG-1.x- sind PCISA-CPU-Slotkarten nur halb so lang. Beim Stecker stand der für EISA Pate, allerdings mit neuer Belegung. Wie dort ist aber der obere Teil für den ISA-Bus reserviert, PCI liegt auf der Verlängerung. Für EISA eignen sich die Karten nicht.

Die Auswahl an Gehäusen und Backplanes für PICMG ist groß. Sie reicht im 19-Zoll-Bereich von 1 bis 6 U. Es gibt einen Erweiterungsplatz für bis zu 19 verfügbaren Slots. Gehäuse zur Wandmontage oder aus Edelstahl sind ebenfalls erhältlich. Wie bei den PCI-Karten kann man bei den Netzteilen auf handelsübliche Ware im AT/ATX-Format zurückgreifen. Als Alternative kommen nicht gekapselte Open-Frame-Netzteile, redundante Lösungen oder eine Gleichspannungseinspeisung mit 12 oder 48 Volt infrage.

Da bereits eine VoIP-TK-Anlage neue und hohe Anforderungen an die Verfügbarkeit stellt, lohnt es sich, Industrie-PCs in Erwägung zu ziehen. Dort finden sich Rechner mit ausreichender Anzahl von Steckplätzen, mit integrierter Watchdog-Überwachung, Gleichspannungsversorgung und passenden Edelstahlgehäusen mit Staubfilter. Nicht zu vergessen die Strom sparenden CPUs und die Liefergarantie für fünf Jahre. (rh)

AXEL URBANSKI

ist freier IT-Berater.

Onlinequellen

[a]	Pentium-M-Board	de.kontron.com/products/boards+and+mezzanines/pc104+sbc+and+peripherals/mops+pc104+cpu+modules/mopspm.html
[b]	PC104-Norm	www.pc104.org
[c]	PICMG-Definitionen	www.picmg.org
[d]	Industrie-Boards	www.amc-systeme.de/de/produkte/industrie_computer___systeme_u__komponenten/de/produkte/industrie_computer___systeme_u__komponenten/ipc_prozessorkarten_u_zubehoer/industrial_motherboards.html
[e]	ATCA-Norm	www.intel.com/technology/atca
[f]	ATCA-Produkte	www.sun.com/products-n-solutions/hw/networking/atca/index.jsp
[g]	ATCA und Telko	www.itwissen.info/definition/lexikon/AdvancedTCA-ATCA-advanced-telecom-computing-architecture.html
[h]	StarFabric	www.starfabric.org







Studien zur Einkommensentwicklung

Manchmal mehr

Achim Born

Der Trend aus dem vergangenen Jahr hat Bestand: Der Mangel an Fachkräften führt nicht automatisch zu überdurchschnittlichen Zuwächsen auf der Gehaltsseite. Beklagen müssen sich die IT-Profis übers Salär indes nicht. Und für das laufende Jahr erwarten die Gehaltsexperten noch einmal einen ordentlichen Zuschlag.

Die Gesamtbezüge von Vorständen deutscher Unternehmen sind im Geschäftsjahr 2006/2007 durchschnittlich um 17,5 % gestiegen. Zu diesem Schluss kommt die Gummersbacher Unternehmensberatung Kienbaum in ihrem jüngst veröffentlichten Einkommensbericht. Um einer eruptiven Neiddebatte vorzugreifen, sei an dieser Stelle noch schnell die differenziertere Bestandsaufnahme angeführt: Der deutliche Zuwachs ist in erster Linie auf die Erhöhung variabler erfolgsabhängiger Vergütungsbestandteile zurückzuführen, die sich infolge der guten Konjunktur zwangsläufig für die Nutznießer erfreulich entwickelten.

Konsequenterweise wurden andererseits die Vorstandsbezüge im Betrachtungszeitraum bei einem Drittel der Firmen gekürzt, da die Geschäfte hier schlechter liefen. Der Studie zufolge weisen die Bezüge der Vorstandsmitglieder deutscher Aktiengesellschaften zudem eine erhebliche Spanne in der Vergütung auf, die von 40 000 € bis hin zu mehr als sieben Millionen € im Jahr reicht.

Nicht nur von der letztgenannten Summe dürfen IT-Profis nur träumen, dasselbe gilt für den zweistelligen Bezugszuwachs. Denn die rund 43 000 freien Stellen für IT-Spezialisten, die nach Bitkom-Angaben derzeit in Deutschland nach Besetzung verlangen, führten im Allgemeinen noch nicht zu überdurchschnittlichen Steigerungen. Die IG Metall kommt in ihrer jüngsten ITK-Entgeltanalyse sogar zu dem Schluss, dass sich die Gehälter in der Informations- und Telekommunikationsbranche im vergangenen Jahr in der Summe negativ entwickelten.

Näher Hinschauen relativiert Wehklagen

Die Ergebnisse der IG-Metall-Analyse klingen dramatischer, als sie bei eingehender Betrachtung sind. Das liegt zum einen am Erhebungszeitpunkt. Die Daten beziehen sich auf das vierte Quartal 2006. Die deutliche Konjunkturverbesserung in 2007 konnte folglich noch keine Spuren hinterlassen. Zudem sind die einzelnen Werte traditionell auf eine 35-Stunden-Woche normiert, in der Branche gelten jedoch unterschiedliche Wochenarbeitszeiten.

Insbesondere in Vertriebsbereichen ermittelte die ITK-Entgeltanalyse 2008 der IG Metall starke Einbußen. Dabei reduzierten sich die Bonuszahlungen mit bis zu 50 % stärker als die Fixgehälter. Auch in den Bereichen Beratung/Consulting und Servicetechnik sanken die Bruttogehälter um bis zu 13 %. In der Hardwareentwicklung waren sowohl die Gehälter als auch die Beschäftigtenzahlen rückläufig. Ebenfalls negativ zeigte sich der Trend im Bereich Projektmanagement. Positiv hingegen haben sich die Entgelte in den Callcentern entwickelt, wo besonders in der Einstiegsstufe hohe Steigerungen von bis zu einem Drittel zu verzeichnen sind.

Einbußen bei den Hardwareentwicklern

Sowohl für Anfänger als auch für erfahrene Mitarbeiter im Bereich Hardware wird ein Rückgang von mehreren Tausend Euro beim Jahressalär aufgewiesen. Nahm der „gewöhnliche“ Entwickler laut 2007er-Analyse noch durchschnittlich 53 742 € (Fixgehalt plus variable Bestandteile) mit nach Hause, betrug der gewichtete Mittelwert heuer 39 200 €. Für den Juniorentwickler reduzierte sich das Einkommen um circa 14 000 € auf 36 400 €, für den Seniorentwickler sogar um knapp 19 000 € auf 42 500 €. Freuen durfte sich allein der Leiter in der Hardwareentwicklung, dessen Gehalt um 1200 € auf 87 500 € stieg.

Ein Minus wiesen ebenso die Einkommen der Beschäftigten in Rechenzentren auf. Sie muten im Vergleich zur Hardwareentwicklung allerdings weniger drastisch an. Das Gehalt der Operatoren mit langjähriger Berufserfahrung hat sich danach um ein Zehntel auf 44 800 Euro reduziert. Ein Rechenzentrumsleiter (93 000 €) musste sich mit knapp 6000 € weniger begnügen. Deutliche Rückgänge gab es ebenso bei den

Brutto-Jahresgehalt Branchenvergleich

	oberes Quartil[1]	Median[2]	unteres Quartil[3]
Branche Software			
Softwareentwickler 28 – 30 Jahre	50 770 €	44 731 €	40 346 €
Softwareentwickler 35 Jahre	61 355 €	52 500 €	46 016 €
Gruppenleiter 35 Jahre	72 750 €	61 622 €	53 197 €
Abteilungsleiter 40 Jahre (Führung einer Abteilung mit 10 Mitarbeitern)	96 075 €	81 384 €	71 950 €
Bereichsleiter 45 Jahre (Führung eines Bereiches mit 50 Mitarbeitern in mehreren Abteilungen)	138 125 €	119 000 €	106 624 €
Branche IT-Systemhaus			
Softwareentwickler 28 – 30 Jahre	53 000 €	47 355 €	42 433 €
Softwareentwickler 35 Jahre	65 465 €	56 559 €	50 344 €
Gruppenleiter 35 Jahre	72 533 €	62 854 €	55 387 €
Abteilungsleiter 40 Jahre (Führung einer Abteilung mit 10 Mitarbeitern)	90 525 €	82 592 €	76 675 €
Bereichsleiter 45 Jahre (Führung eines Bereiches mit 50 Mitarbeitern in mehreren Abteilungen)	124 320 €	111 000 €	101 256 €
Branche Industrie > 5000 Mitarbeiter			
Softwareentwickler 28 – 30 Jahre	58 500 €	51 900 €	46 688 €
Softwareentwickler 35 Jahre	73 395 €	65 999 €	58 941 €
Gruppenleiter 35 Jahre	79 166 €	71 240 €	63 792 €
Abteilungsleiter 40 Jahre (Führung einer Abteilung mit 10 Mitarbeitern)	101 900 €	91 052 €	81 000 €
Bereichsleiter 45 Jahre (Führung eines Bereiches mit 50 Mitarbeitern in mehreren Abteilungen)	131 150 €	116 230 €	100 322 €

[1] 25 Prozent verdienen mehr
[2] 50 % verdienen mehr, 50 % verdienen weniger
[3] 25 % verdienen weniger
Alle Angaben in Euro

Quelle: Personalmarkt-Vergütungsstudie „IT-Funktionen“, 10/2007

Gehältern der Anwendungsentwickler und leitenden Softwarespezialisten. Erstere erhielten nach IG-Metall-Berechnung mit rund 37 000 € über 8000 € weniger. Bei den leitenden waren dies circa 4500 Euro.

Doch auch in Gewerkschaftskreisen geht man davon aus, dass aufgrund der guten Geschäftslage 2007 und dem Mangel an Fachleuten die Gehaltskurve in den kommenden Jahren „deutlich nach oben zeigt“. Andererseits sind die Gehaltseinbußen zum Teil ein Beleg für die schwindende Bedeutung der Hardwarefertigung in Deutschland.

Andere Analysten, andere Ergebnisse

Gehaltsuntersuchungen von Kienbaum oder Personalmarkt haben im Unterschied zur IG-Metall-Untersuchung die Steigerungen im vergangenen Jahr bereits eingerechnet. So berichtet Kienbaum in der branchenübergreifend angelegten Vergütungsstudie 2007 (Erhebungsstichtag: 1. Februar 2007) von einem durchschnittlichen Plus von 3 % der Jahresgesamtbezüge von Führungs- und Fachkräften der Informationstechnik. Danach lag 2007 das Jahresgesamtgehalt von IT-Führungskräften, die disziplinarische Führungs- und Personalverantwortung gegenüber Mitarbeitern haben, im Schnitt bei 105 000 €. Eine Fachkraft erhielt 60 000 €. Die Angaben setzen sich dabei jeweils aus Jahresgrundgehalt und variablen Vergütungsbestandteilen zusammen. In die Zahlen nicht eingerechnet sind die geldwerten Vorteile von betrieblichen Zusatzleistungen sowie Überstundenvergütungen.

Wie bereits in den Vorjahren registrierte die Kienbaum-Untersuchung einen Trend zur stärkeren Gewichtung der variablen Vergütungskomponenten. Das Gehalt von 78 % aller Führungskräfte und 55 % der Fachkräfte enthielt 2007 einen variablen Bestandteil in Form von Prämien, Tantiemen, Boni oder sonstigen Sonderleistungen. Im Vorjahr betrug die durchschnittlich ausgeschüttete Höhe 17 900 € für eine Führungskraft und 6800 € für eine Fachkraft. Neben dem Gehalt bilden betriebliche Zusatzleistungen, etwa die betriebliche Altersversorgung, Arbeitgeberdarlehen oder Ähnliches, einen gewichtigen Faktor des Vergütungssystems. Diese Leistungen entsprechen oft erheblichen finanziellen Äquivalenten, sie sollten deshalb beim Gehaltsvergleich einbezogen werden.

iX-TRACT

- Die hohe Nachfrage nach IT-Fachkräften führte bislang noch nicht zu exorbitanten Gehaltssteigerungen.
- Variable Einkommensbestandteile gewinnen an Einfluss.
- Vor allem Projektleiter dürfen sich über gestiegene Einkommen freuen.

Zweifelsfrei die höchsten Jahresgesamtbezüge erzielten nach der Gehaltsstatistik von Kienbaum im vergangenen Jahr die Leiter Informationsverarbeitung und Organisation mit einer Spannweite von 98 000 € (unteres Quartil) und 163 000 (oberes Quartil). Für den Leiter IT-Management lauten die Vergleichszahlen 97 000 und 134 000 Euro. Die Einkommensunterschiede für IT-Fachkräfte fielen in der Relation ähnlich hoch aus. Im Bereich der Anwendungsentwicklung lagen die Einkommen beispielsweise in der Bandbreite von 46 000 € und 62 000 €.

Zu den wichtigen Einflussfaktoren auf die Gehaltshöhe zählt der jeweilige Standort. Wie in der Vergangenheit ergab sich, dass die Vergütung in den großstädtischen Ballungsräumen am höchsten ausfällt. Das 2007er-Niveau der Jahresgesamtbezüge von IT-Kräften in den neuen Bundesländern belief sich im Durchschnitt auf knapp 80 % der in Deutschland gezahlten Gehälter. Ursache ist unter anderem die größere Konkurrenz der Unternehmen in Ballungsgebieten um einzelne Mitarbeiter. Auf der anderen Seite stellt das Mehr an Einkommen oftmals auch „nur“ ein Äquivalent für die höheren Lebenshaltungskosten in den Zentren dar.

Betriebsgröße beeinflusst Chef-Honorar

Einen erheblichen Einfluss auf die Vergütungsstruktur (vgl. Tabelle: Alter und Firmenumsatz beeinflussen Jahresgesamtbezüge) üb(t)en neben positions- und personenspezifischen Aspekten unternehmensbezogene Faktoren aus. So steigt die Personalverantwortung tendenziell mit der Größe des Unternehmens und der Abteilung. Mehr Verantwortung ist indes in der Regel gleichbedeutend mit mehr Gehalt. Ein

Jahresgesamtbezüge nach Alter und Firmenumsatz

Position	bis 30 J.	30 bis 35 J.	35 bis 40 J.	40 bis 45 J.	45 bis 50 J.	50 bis 55 J.	über 55 J.	bis 15 Mio. Euro	15 bis 50 Mio. Euro	50 bis 100 Mio. Euro	100 bis 250 Mio. Euro	250 bis 500 Mio. Euro	500 bis 1000 Mio. Euro	über 1000 Mio. Euro	Durchschnitt Euro
Leiter IT Management	–	76	93	99	117	141	140	91	95	102	113	116	128	157	115
Leiter Anwendungsentwicklung	–	–	84	100	105	101	109	78	94	103	100	102	104	110	102
Leiter IT Betrieb	–	–	74	93	92	95	110	79	79	80	80	91	104	107	93
Leiter Netzwerktechnik/ TK	–	81	75	88	94	111	–	62	69	69	75	–	99	98	87
Projektleiter	51	69	72	72	79	77	92	71	70	72	73	–	75	80	73
Datenbankdesigner	49	44	59	63	73	73	74	60	62	64	65	–	66	68	65
Anwendungsentwickler	39	48	55	60	59	64	66	45	51	49	51	52	55	61	55
Webredakteur	–	49	53	52	55	70	78	49	50	47	–	57	61	65	58
Systemprogrammierer	40	56	59	62	64	74	66	–	55	56	56	62	59	64	61
Helpdesk-Spezialist	36	43	44	49	46	51	55	34	44	46	47	46	51	47	45

Angaben in Euro, J. = Jahre

Quelle: Vergütungsstudie 2007, Kienbaum

Leiter des IT-Managements erhielt in einem Betrieb mit bis zu 100 Mitarbeitern ein durchschnittliches Jahresgehalt von 95 000 Euro. Auf der gleichen Position hätte er in einem Unternehmen mit über 5000 Mitarbeitern durchschnittlich 169 000 Euro im Jahr verdient. Arbeitet er in einem kleineren Betrieb mit einem Jahresumsatz von bis zu 15 Mio. €, wurde er mit 91 000 € entlohnt. Die Gesamtjahresbezüge von Leitern des IT-Managements in Großunternehmen (über 1 Mrd. Euro Jahresumsatz) beliefen sich dagegen auf 157 000 €.

Im Falle der IT-Fachkräfte waren die Gehaltsunterschiede bei identischer Position nicht ganz so dramatisch. Hier zählte eher die Berufserfahrung – und damit indirekt auch das Lebensalter. Es gilt nach wie vor die Daumenregel, dass das Einkommen mit dem Alter steigt. Ein Anwendungsentwickler jenseits der 55 durfte sich der Kienbaum-Untersuchung zufolge schon einmal über 66 000 Euro Gehalt freuen, während sein junger Kollege (unter 30 Jahre) sich mit 39 000 € begnügen musste.

Zu beachten ist laut Studienautoren allerdings, dass zum Stichtag der Untersuchung die seinerzeit noch „maue“, konjunkturelle Lage für stagnierende oder zum Teil rückläufige Durchschnittsgehälter in der Altersklasse „bis 30 Jahre“ sowie in der Firmen- beziehungsweise Positionszugehörigkeit führte. Angesichts der verbesserten wirtschaftlichen Gesamtsituation darf man in diesem Punkt eine arbeitnehmerfreundlichere Entwicklung erwarten. Zumindest geht Kienbaum im Vorfeld der Neuauflage der Untersuchung allgemein von einem verbesserten Gehaltsplus aus. Dies soll in Unternehmen, die die Gehaltsrunde am 1. Februar bereits hinter sich hatten, bei 3,5 % liegen. Mitarbeiter von Firmen, in denen die Erhöhung noch

im Laufe des Jahres erfolgt, sollen sich sogar auf ein Plus von 3,8 % freuen dürfen.

Ausgleich für müdes Vorjahr

Die Hamburger Vergütungsberatung Personalmarkt veranschlagt in einer gemeinsam mit der Computerwoche durchgeführten Auswertung das Plus sogar noch ein wenig höher. In der Ende Februar veröffentlichten Untersuchung wird branchenübergreifend für das laufende Jahr von einer 4%igen Gehaltssteigerung für IT-Chefs ausgegangen. Dieser Zuwachs nimmt sich noch bescheiden aus, da die Berufsgruppe der Projektleiter ein doppelt so hohes Plus erzielen soll. Als Erklärung für diesen Gehaltssprung führt Personalmarkt die Stagnation aus dem Vorjahr an, die nun ein wenig ausgeglichen werde.

Konkret hat sich das Bruttogehalt der Projektleiter mit Personalverantwortung um knapp 7000 € auf 88 000 € erhöht. Fehlt die disziplinarische Zuständigkeit, ist noch immer ein Plus von 5000 € auf 65 000 € zu verzeichnen.

Die Personalmarkt-Statistik deckt zudem einen erheblichen Einfluss der Branche auf die positionsbezogenen Einkommen auf (siehe auch Tabelle „Brutto-Jahresgehalt im Branchenvergleich“). Wer in der Finanzbranche schafft, darf sich allgemein über das höchste Salär freuen. So nimmt ein dort beschäftigter Projektleiter durchschnittlich 80 750 € mit nach Hause. Die Kollegen in der Telekommunikationsindustrie kommen hingegen auf 73 326 €. In der Automobilbranche werden 70 357 € verdient. Projektleiter von System- und Softwarehäusern erhalten 65 394 € beziehungsweise 59 758 €. Ein IT-Bereichsleiter in der Finanzwirtschaft erhält durchschnittlich 165 000 € im Jahr, während in den System- und Softwarehäusern die Bereichsleiter „nur“ 108 000 beziehungsweise 105 000 € verdienen. Zu beachten ist allerdings, dass die „softe“ IT-Branche eher mittelständisch geprägt ist. Folglich fällt das Gehalt auch aufgrund der Firmengröße geringer aus.

Die Hamburger Vergütungsberatung dokumentiert in einer eigens für diese Zeitschrift durchgeführten Auswertung auf Basis von knapp 9000 Datensätzen zudem die enge Korrelation von Gehalt und Alter (vergl. Tabelle „Alter zahlt sich aus“). Das Einkommen eines 25-jährigen Projektleiters liegt demnach zwischen 38 400 € (unteres Quartil) und 49 737 € (oberes Quartil). Bei den 35-Jährigen lauten die Vergleichswerte 57 047 € und 72 000 €, bei den 55-Jährigen 70 200 € und 90 050 €.

Unter dem Strich belegen die zitierten Gehaltsstatistiken die vielfältigen Einflussgrößen, die auf eine Gehaltsgestaltung wirken. Neben unternehmensbezogenen Faktoren wie Größe, Umsatz oder Branche, positionsspezifischen Aspekten und eigener Berufserfahrung sollten auch Markteinflüsse nicht vernachlässigt werden. Die Berater sind sich im Groben einig, dass die hohe Nachfrage mit großer Wahrscheinlichkeit – zumindest diesmal noch – in höheren Abschlüssen mündet. Wer darüber hinaus Spezialkenntnisse etwa im SAP-Umfeld aufweist, kann durchaus noch einen weiteren Gehaltsaufschlag aushandeln. (JS)

Alter zahlt sich aus

nach Alter/Funktionen ohne Personalverantwortung	oberes Quartil	Median	unteres Quartil
Softwareentwickler			
25 Jahre	43 600 €	39 600 €	36 000 €
30 Jahre	51 268 €	47 560 €	42 600 €
35 Jahre	61 355 €	52 500 €	46 016 €
40 Jahre	62 160 €	53 266 €	47 260 €
45 Jahre	64 700 €	54 100 €	48 288 €
50 Jahre	67 850 €	56 270 €	49 620 €
55 Jahre	71 586 €	59 860 €	49 800 €
IT-Berater			
25 Jahre	45 009 €	42 000 €	38 035 €
30 Jahre	56 400 €	48 700 €	43 537 €
35 Jahre	68 651 €	59 477 €	53 000 €
40 Jahre	73 560 €	64 000 €	56 438 €
45 Jahre	81 970 €	70 649 €	62 073 €
50 Jahre	83 900 €	72 000 €	61 000 €
55 Jahre	80 300 €	72 000 €	65 256 €
Projektleiter			
25 Jahre	49 737 €	42 000 €	38 400 €
30 Jahre	63 000 €	54 000 €	47 250 €
35 Jahre	72 000 €	63 950 €	57 047 €
40 Jahre	80 275 €	71 056 €	63 000 €
45 Jahre	87 500 €	76 210 €	66 867 €
50 Jahre	85 099 €	75 282 €	66 249 €
55 Jahre	90 050 €	77 750 €	70 200 €

Quelle: Personalmarkt-Vergütungsstudie „IT-Funktionen“, 10/2007

Entwicklung der Jahresgehälter *)

Funktion	2007	2006	2005
Juniorberater	44 325	42 881	45 833
Berater	53 957	57 247	56 490
Seniorberater	64 899	69 109	74 470
Chefberater	73 432	88 039	108 200
Manager	83 384	98 640	110 812
HRW-Juniorentwickler	36 400	50 234	41 867
HRW-Entwickler	39 200	53 742	47 714
HRW-Seniorentwickler	42 467	61 113	56 851
Gruppenleiter Entwicklung Hardware	65 625	74 619	71 138
Leiter Entwicklung Hardware	87 455	86 139	74 077
Sfw-Entwickler-Junior	37 033	45 183	43 912
Sfw-Entwickler	54 209	55 208	57 887
Sfw-Entwickler-Senior	60 471	66 417	65 074
Leiter Software Engineering	92 270	100 752	82 969

*) Jahr der Erhebung, gewichteter Mittelwert
Alle Angaben in Euro gerundet, 35-Std.-Basis

Quelle: IG Metall, 03/2008

Literatur

[1] Entgelt in der ITK-Branche 2008, 10. Erhebung, IGM Metall, knapp 20000 Datensätze aus 26 Betrieben

[2] Vergütungsstudie „Führungskräfte und Spezialisten in IT-Funktionen 2007/2008“, PMSG Personalmarkt Services GmbH, 19486 Daten in 26 Funktionen

[3] Vergütungsstudie Führungs- und Fachkräfte in der Informationstechnologie 2007“, 34. Ausgabe, Kienbaum Management Consultants GmbH, 5682 Einzelpositionen aus 192 Unternehmen



Vom unrealistischen Hype zum vorsichtigen Optimismus

Berührungslos

Barbara Lange

Berührungslose Funktechnik kennt viele Einsatzbereiche: Am bekanntesten ist sie bei Handel und Logistik, aber auch andere Branchen wie Luftfahrt, Automobilindustrie oder Pharma setzen auf RFID – und jede Branche stellt eigene Ansprüche an Transponder und Systeme. Ein Rundumschlag.

Der Hype hat sich gelegt. RFID habe teilweise unrealistische Hoffnungen auf einen schnellen und umfassenden Einsatz geweckt, so die Einschätzung von Branchenkennern [1]. Von einem vorsichtigen Optimismus sprechen auch die Marktforscher von Abi Research. Große RFID-Systeme entwickelten sich demnach nicht ganz so schnell wie vermutet. Insgesamt aber prognostizieren die Autoren von Studien sowie Marktforscher von Abi Research und Gartner ein weltweites Umsatz-Wachstum im RFID-Umfeld zwischen 20 und 30 Prozent.

Handel und Logistik treiben RFID voran, schrieb *iX* vor zwei Jahren [2]. Das stimmt noch immer. So wandert die berührungslose Funktechnologie kontinuierlich von Paletten über Kartons langsam auch auf die einzelnen Artikel.

Für die Ebene der Paletten meldete die Metro Group (www.future-store.org) Ende vergangenen Jahres den größten operativen Einsatz von RFID im europäischen Handelssektor: Alle 80 Cash&Carry-Großmärkte in Deutschland und 100 Real-SB-Warenhäuser erhielten RFID-Wareneingangstore, die die mit Tags bestückten Versandpaletten viel schneller, als es mit den Hand-Scannern möglich war, einlesen und innerhalb von Sekunden automatisch prüfen können, ob eine Lieferung vollständig ist.

Im laufenden Jahr sollen noch 200 Standorte mit Lesegeräten am Wareneingangstor ausgestattet werden, gab das Unternehmen auf der Cebit bekannt. Zur weiteren Optimierung ist eine Integration von Temperatursensoren geplant, mit deren Hilfe man überprüfen will, ob die Kühlkette bei leicht verderblichen Lebensmitteln während des Transports nicht unterbrochen wurde.

Umfassender Einsatz dauert noch

Allein durch die Verwendung von RFID auf Paletten kann Metro rund 8,5 Millionen Euro pro Jahr einsparen. Und auch der globale Einsatz läuft. Seit Ende 2007 versehen 100 Hersteller aus China und Vietnam ihre Exportkartons im Rahmen des Pilotprojekts „Tag it Easy“ mit RFID-Transpondern. Aus Sicht der Metro gibt es noch einige Herausforderungen zu meistern: Dazu gehört das weitere Vorantreiben von globalen einheitlichen Standards für Frequenzen und Daten, bezahlbaren technischen Lösungen, Lesegeräten und Transpondern.

Bis der Konsument tatsächlich seinen vollen Einkaufswagen durch den RFID-Lesebereich der Supermarkt-Kasse schieben kann, dauert es wohl noch 10 bis 15 Jahre, zumal es noch Schwierigkeiten beim Einlesen von Artikeln mit Flüssigkeiten oder Metall gibt. Branchenkenner schätzen derzeit, dass RFID sich zunächst im Handel bei teuren Produkten und im Bereich Textil durchsetzen wird.

Zu sehen ist dies derzeit in der Herrenabteilung von Galeria Kaufhof in Essen. Hier befinden sich die Funkchips seit September 2007 auf den einzelnen Artikeln – sogenanntes Item-Tagging im Pilotstadium. Lesegeräte stehen an allen Ein- und Ausgängen sowie an Rolltreppen der Etage. So lässt sich jederzeit ermitteln, wo sich welches Produkt gerade befindet und ob der Pullover vielleicht noch in anderer Farbe oder Größe auf einem anderen Tisch liegt.

Als großen Vorteil nennen die Betreiber eine hohe Warenverfügbarkeit durch einen ständigen Abgleich mit dem Warenwirtschaftssystem. Auch der Kunde habe Vorteile, denn er erhalte



RFID auf Artikelebene in der Herrenabteilung der Galeria Kaufhof in Essen. Die „intelligente Umkleidekabine“ gibt Zusatzinformationen zum gewählten Produkt (Abb. 1).

Zusatzinformationen über das Produkt: zum Beispiel über mögliche Farbkombinationen, die ihm eine „intelligente Umkleidekabine“ (Abb. 1) mitteilt.

Aber auch der gute alte Barcode wird in einigen Szenarien erhalten bleiben, denn RFID ist nur eine von mehreren AutoID-Techniken, was auf der Cebit etwa durch den Begriff „Auto-ID/RFID-Solutions Park“ zum Ausdruck kam. So gibt es im Handel derzeit Überlegungen, ab 2010 den von EPCglobal (Electronic Product Code; www.epcglobalinc.org) standardisierten erweiterten Barcode namens „GS1 DataBar“ global einzuführen. Vorteile: Er verfügt über mehr Speicherplatz als der herkömmliche Barcode und kennt sowohl das Datum für die Mindesthaltbarkeit als auch das Gewicht von abgepackten Lebensmitteln.

2D verbindet Online- mit Offline-Welt

Darüber hinaus machen sich derzeit 2D-Barcodes auf den Weg, die Online- und Offline-Welt zu vernetzen [3]. Wird das Handy dann zum Lesegerät, hätte es gleichzeitig ein Display – was viele bislang im RFID-Bereich immer vermissten.

Wenn Konsumenten direkt mit RFID in Berührung kommen, zeigt sich das Spannungsfeld dieser unsichtbaren Funktechnik im Konflikt zwischen der Optimierung der Logistik und einer bedrohten Privatsphäre durch Funkchips, die unbemerkt Transaktionen speichern und in undurchsichtigen Hintergrundsystemen ablegen können – ein Grund, warum Bundesdatenschützer Peter Schaar nicht müde wird, das Bedrohungspotenzial von RFID zu thematisieren. Im Zusammenhang mit Vorratsdatenspeicherung, ubiquitärem Computing, Biometrie und Videoüberwachung entstehen gruselige Szenarien [4].

Seine Forderung: Datenschutz und Sicherheit müssen von vornherein in die Technik integriert sein und nicht hinterher aufgepfropft werden. Derzeit fehlt es aber noch an der Hardware-Sicherheit, wie unter anderem die Studie „RFID-Studie 2007 – Technologieintegrierte Datensicherheit bei RFID-Systemen“, des Fraunhofer-Instituts für Sichere Informationstechnologie (SIT) und anderen feststellt (siehe Kasten „Onlinequellen“, [a]). Auf preisgünstigen Chips gibt es keine Kryptografie, auch nicht auf dem von EPCglobal standardisierten Transponder „EPC Class1 Gen2-Tag“ oder zwischen Lesegerät und Tag.

iX-TRACT

- RFID hat in einzelnen Branchen einen eigenen Entwicklungsstand. In geschlossenen Kreisläufen wird es seit Jahrzehnten eingesetzt, zum Beispiel in der Produktion.
- Für offene Kreisläufe sind branchenübergreifende Standards erforderlich. Der Standard „EPC Class1 Gen2“ definiert die Luftschnittstelle für den Austausch mit dem Lesegerät und die Datenstruktur auf dem Transponder. Die branchenübergreifende Verwendung einheitlicher Nummernsysteme ist schwierig umzusetzen.
- Im konsumentennahen Einsatzbereich sehen staatliche Stellen derzeit keinen Regulierungsbedarf, Vorschläge zu datenschutzfreundlichem RFID-Einsatz existieren aber.

Inwieweit die Verantwortlichen in Politik und Wirtschaft Forderungen wie Datenvermeidung und Datensparsamkeit erfüllen werden oder wollen, bleibt fraglich. Dass RFID bis mindestens 2010 überwiegend eine Hintergrundtechnik bleiben wird, die den Konsumenten nicht direkt betrifft, haben die Teilnehmer der europäischen Konferenz „Towards the Internet of Things“ festgestellt, die die Bundesministerien für Wirtschaft und Forschung sowie die Europäische Kommission Mitte letzten Jahres in Berlin ausgerichtet haben. Eine weitere Konferenz ist für den kommenden November angekündigt.

Selbstregulierter Persönlichkeitsschutz

Bislang ist es bei dieser Einschätzung geblieben, wie die Bundesregierung Mitte Februar 2008 in einer „Unterrichtung“ [b] mitteilte: Da RFID-Systeme noch keine Verbreitung im datenschutzrelevanten Bereich gefunden haben, soll die Industrie die Persönlichkeitsrechte der Konsumenten auf der Basis von Selbstregulierung schützen. Gesetzliche Vorgaben soll es nicht geben.

Auch die EU-Kommission setzt auf eine Selbstregulierung der Industrie, differenziert aber in einem Entwurf die Bewältigung von Datenschutzproblemen [c]. Den Entwurf, der seit Februar online veröffentlicht ist, konnten Bürger, Unternehmen und Organisationen bis Ende April kommentieren. Die vorgeschlagenen Regeln: Betreiber von RFID-Systemen sollen vor der Implementierung abschätzen, welche Folgen der Einsatz für die Nutzer hat – ist es etwa möglich, eine Person mit den gewonnenen Daten zu überwachen? Weiterhin schlägt die Kommission vor, RFID-Lesebereiche und Produkte einheitlich zu kennzeichnen. Der Konsument müsse die Gelegenheit erhalten, den RFID-Chip zu deaktivieren.

Vor einer gesetzlichen Verankerung dieser Wahlmöglichkeit der Deaktivierung von RFID-Chips warnte indes das Informationszentrum RFID (www.info-rfid.de) auf der Cebit. Begründung: Dies würde die Wettbewerbsfähigkeit der europäischen Wirtschaft behindern, zu teuere Chips hervorbringen und den Konsumenten daran hindern, Vorteile beispielsweise bei der Garantieabwicklung zu nutzen. Mitglieder des Informationszentrums RFID sind weltweit führende Unternehmen aus den Bereichen Handel, Konsum-

güterindustrie, Automobilbranche, IT und Dienstleistung.

Einen Mittelweg schlägt derzeit das Bundesamt für Sicherheit in der Informationstechnik (www.bsi.de) ein. Gemeinsam mit NXP Semiconductors erarbeitet das BSI „Technische Richtlinien für den sicheren Einsatz von RFID“ (TR). In vier Szenarien mit potenziellem Konsumentenkontakt sollen die Richtlinien RFID ein vergleichbares Sicherheitsniveau ermöglichen: E-Ticketing mit und ohne Near Field Communication (NFC), das Event-Ticketing bei Veranstaltungen sowie der Einsatz in Handel und Logistik.



Bahn modern: Das Einlesen des Start- und Zielortes einer Bahnreise via Handy erspart das Schlangestehen am Ticketschalter. Bezahlt wird später per Rechnung (Abb. 2).

BSI erarbeitet technische Richtlinien

Referenz-Implementierungen für das Ticketing sind zum einen die Eintrittskartenvergabe der Weltmeisterschaft 2006 und das Projekt Touch&Travel der Deutschen Bahn, das derzeit Test-Fahrgästen einen mobilen Fahrkarten„kauf“ via NFC-Handy ermöglicht (Abb. 2). Dazu lesen die Handys den Anfangs- und Zielort am Bahnhof ein. Aus diesem Themenspektrum fällt das vierte Szenario „Handel und Logistik“ etwas hinaus, weshalb man im BSI wohl auch zu Redaktionsschluss noch daran arbeitete.

Das BSI verfolgt mit der TR RFID den Anspruch, als neutrale Stelle eine Richtlinie herauszubringen, die den sicheren Einsatz von RFID unterstützt und die Privatsphäre der Konsumenten schützt. Darüber hinaus hofft man die Aufnahme in europäische Empfehlungen.

Als alles durchdringende Querschnittstechnik misst auch die Bundesregierung der berührungslosen Funktechnik eine große Bedeutung zu und fördert vier Projekte, die neue Geschäftsfelder erschließen sollen: Ko-RFID, LAENDmarKS, LogNetAssist und Sm@rtLogistics. Die Projekte sind Teil des auf dem IT-Gipfel 2006 und 2007 definierten Leuchtturmvorhabens „Internet der Dinge“ (www.nextgenerationmedia.de). Eine große Rolle spielt dabei die Automobilindustrie,



In der Automobilfertigung ist der RFID-Einsatz in geschlossenen Systemen von Vorteil und längst üblich: Die in den Schutzkästchen befindlichen wiederverwertbaren Tags kennen den Produktionsstatus jedes Fahrzeugs. Bei Störungen kann man so anschließend wieder an der richtigen Stelle fortfahren (Abb. 3).

wobei man auch die Übertragbarkeit auf andere Branchen wie Luftfahrt oder Medizin prüft. Das mit 5 Millionen Euro geförderte Projekt Ko-RFID untersucht, wie global und firmenübergreifend kooperierende Unternehmen Kosten, Nutzen und Risiken fair aufteilen können (siehe auch Bericht S. 21). Darüber hinaus wollen die Kooperationspartner – dabei sind SAP, Gerry Weber, DaimlerChrysler und der Küchenhersteller Wellmann – herausfinden, wo die Daten am besten zu speichern sind: auf dem Tag oder in dahinter liegenden Netzwerken.

Neue Geschäftsfelder in Erprobung

Um eine schnelle Rückverfolgbarkeit sicherheitsrelevanter Automobilkomponenten geht es im Projekt LAENDmarKS. Die Projektbeteiligten, darunter DaimlerChrysler, Volkswagen und IBM, wollen ein Nachverfolgungssystem aufbauen, das alle Beteiligten informiert, wenn fehlerhafte Teile im Umlauf sind – und zwar vor dem Einbau.

Ein audiovisuelles Assistenzsystem entsteht im Projekt LogNetAssist (Bosch, Siemens, Daimler und das Fraunhofer-Insitut IML). Eine multimediale Visualisierung des Warenflusses soll Entscheidungshilfen zur Steuerung von Logistikprozessen geben.

Und last but not least gehört zu den neuen Betätigungsfeldern Sm@rtLogistics, ein RFID-gestütztes Produktions- und Beschaffungslogistiksystem für die Automobilzulieferindustrie. Dabei geht es darum, die Mitarbeiter bei der Materialversorgung optimal einzusetzen. Auch wird für jeden Auftrag die Beladung der Transportmittel neu berechnet. Projektbeteiligte sind die Intellion AG, die RWTH Aachen, die simcron GmbH, die TU Dresden und die tedrive Germany Gmbh.

Branchenspezifische Anforderungen

Dass man jede Branche und jeden Einsatzbereich von RFID genau untersuchen muss, um zu angemessenen Anwendungen zu kommen, ist Konsens. So sind Ansprüche, Bedingungen und historische Entwicklung der RFID-Nutzung in der Automobil- und Luftfahrtindustrie etwa ganz andere als im Handel, zum Beispiel in Bezug auf die Sicherheit sowie die Speicherfähigkeit und Leistung der Transponder.

Auch ist noch nicht ganz klar, inwieweit die einzelnen Branchen den Ende 2004 von EPCglobal standardisierten „EPC Class1 Gen2 Tag“ nutzen werden oder eigene Standards verwenden. Der Gen-2-Tag, der die Luftschnittstelle für den Austausch mit dem Lesegerät und die Datenstruktur auf dem Transponder für den Electronic Product Code (EPC) definiert, versteht sich zwar branchenübergreifend und ist in die ISO-Norm 18000-6C eingeflossen, kommt aber überwiegend im Handel zum Einsatz.

Als erster Automobilhersteller trat Daimler im November 2007 der Standardisierungsorganisation EPCglobal bei und beteiligt sich dort an der Entwicklung von RFID-Standards auch für die Automobilindustrie, was besonders für global vernetzte Material- und Produktionsströme über Unternehmensgrenzen hinweg wichtig wird.

Noch betreibt die Automobilindustrie derzeit überwiegend RFID-Systeme in der Fertigungsumgebung und Pilotprojekte im Logistikbereich. Seit Anfang der 80er-Jahre steuert RFID die Produktion und hat sich dort in geschlossenen Systemen mit hochwertigen wiederverwendbaren Transpondern etabliert (Abb. 3). Das betont Holger Schönherr, Leiter des Kompetenz-Centers RFID bei Siemens Industry Automation in einem Gespräch mit *iX*. Nach wie vor sei der größte Einsatzbereich in geschlossenen Kreisläufen zu finden, in denen RFID-Systeme vollständig integriert sind. Die Bearbeitungsschritte werden auf dem Tag am Objekt gespeichert, was unter anderem die Wiederaufnahme der Produktion bei Störungen sehr erleichtert. Diese mobile Datenspeicherung am Objekt erweist sich vor allem für die variantenreiche Produktion als wichtig, da sich hieraus entscheidende Wettbewerbsvorteile ergeben, so Schönherr.

Wichtig ist RFID auch aufgrund der steigenden Komplexität in den industriellen Lieferketten. Der Endkunde kann sich sein Automodell individuell zusammenstellen – eine Herausforderung für die Bereitstellung der richtigen Bauteile zur richtigen Zeit am richtigen Ort.

Verwendung eigener Nummernsysteme

Ging es zunächst primär um die Datenspeicherung an Objekten, werden jetzt Schritte getan in Richtung einer automatischen Identifizierung von Bauteilen und ihrer Verfolgung über die ganze Lieferkette hinweg. Dabei spielt auch besagter Gen-2-Tag von EPCglobal eine Rolle. Woran man sich hält, ist der standardisierte Datenaustausch mit dem Reader. Aber welche Daten man in welcher Struktur auf den Transponder schreibt, das bleibt Sache der Automobilhersteller.

Auch die Luftfahrtindustrie verwendet eigene historisch gewachsene Nummerierungen für ihre Teile, die sich nicht so einfach mit dem Electronic Product Code aus Handel und Logistik vereinbaren lassen. Innerhalb

der Air Transport Association (ATA) arbeitet man derzeit an der Definition der Datenstruktur, die man auf dem Transponder speichern will. Die von EPCglobal standardisierte Luftschnittstelle will die Industrie aber berücksichtigen.

Für den Einsatz von RFID im Flugzeug bei der Wartung hochwertiger Teile gibt es eine zusätzliche Anforderung: Der Transponder benötigt eine hohe Speicherkapazität, da man auch hier die Daten lokal ablegen will, muss hohe Temperaturschwankungen aushalten und resistent sein gegen Umprogrammierungsversuche von Fahrgästen. Ein solcher Chip ist derzeit noch nicht verfügbar. Ob sich der Anfang des Jahres von Fujitsu veröffentlichte Chip mit einer Speicherkapazität von 64 Kilobyte eignet, muss sich zeigen.

Fazit

Der RFID-Einsatz läuft unaufhörlich, wobei es deutliche Unterschiede in den einzelnen Branchen gibt. Inwieweit die branchenübergreifende Standardisierung fortschreiten wird, scheint derzeit noch nicht absehbar. Was darüber hinaus noch fehlt, sind Transponder mit großer Speicherkapazität und autonomer Energieversorgung, zusätzlichen Displays und kryptografischen Sicherheitsmaßnahmen.

Neue Anwendungen entstehen durch die Integration von Sensoren in RFID-Systeme, die Temperatur, Erschütterungen oder die Luftfeuchtigkeit messen. So wird beispielsweise eine Überwachung der Temperatur im Lebensmittelbereich möglich. (ur)

Onlinequellen

[a] RFID-Studie 2007 – Technologieintegrierte Datensicherheit bei RFID-Systemen
www.sit.fraunhofer.de/Images/RFID-Studie2007_tcm105-98165.pdf

[b] Unterrichtung durch die Bundesregierung
dip21.bundestag.de/dip21/btd/16/078/1607891.pdf

[c] EU-Entwurf zum Datenschutz
ec.europa.eu/information_society/policy/rfid/doc/consde.pdf

BARBARA LANGE

ist IT-Journalistin und Inhaberin des Redaktionsbüros kurz&einfach in Lengede.

Literatur

[1] Frank Gillert, Wolf-Rüdiger Hansen; RFID – Für die Optimierung von Geschäftsprozessen; Hanser, München 2007

[2] Barbara Lange; RFID; Aufbruchsstimmung; RFID-Systeme in Handel und Logistik; *iX* 3/2006, S. 88

[3] Klaas Wilhelm Bollhoefer; Alles klickt; Der mobile Link ins Internet – 2D-Barcodes; *iX* 3/2008; S. 116 ff.

[4] Peter Schaar; Das Ende der Privatsphäre; Bertelsmann, München 2007







Herstellerunabhängiges Reporting mit XSL und Co.

Der saubere Weg

Markus Karg, Sebastian Krebs

Für ein anspruchsvolles Reporting benötigt man nicht unbedingt teure Software. Professionelle Ergebnisse sind dank der offenen Standards XSL und SVG selbst mit einfachen Open-Source-Werkzeugen zu erzielen. Benutzerfreundlichkeit fügt der kommerzielle Digiforms Designer hinzu.



Viele Unternehmen binden sich an ein proprietäres Produkt, um Reports zu erstellen. Die dadurch entstehende Herstellerunabhängigkeit kann sich mittelfristig als technisch unflexibel herausstellen. Eine Hinwendung zu offenen Standards und freien Werkzeugen ist in diesem Zusammenhang nicht zuletzt eine betriebswirtschaftlich getriebene Entscheidung.

Für das Berichtswesen erforderliche Software besteht üblicherweise aus einem Designwerkzeug zur Erstellung von Berichtsvorlagen sowie einer Runtime-Engine, die mit diesen Berichtsvorlagen aus Rohdaten-Dateien Berichte auf dem Bildschirm sowie auf dem Drucker ausgeben kann. Als nachteilig kann sich erweisen, wenn das Designwerkzeug nur mit beschränkten WYSIWYG-Fähigkeiten ausgestattet ist und die Runtime-Engine nur für Windows zur Verfügung steht. Außerdem müssen in solchen Fällen Druckvorlagen und der Eingangs-Datenstrom in einem proprietären Format vorliegen.

Ein Tausch des Designwerkzeugs oder der Runtime-Engine gegen Produkte konkurrierender Hersteller kann schwierig sein. Im Rahmen der Portierung der betriebswirtschaftlichen Rahmenanwendung auf die Java-Plattform und des damit einhergehenden Paradigmenwechsels (Plattformunabhängigkeit und Unterstützung allgemein akzeptierter Standards) stellte sich für die Autoren die Frage der Nachfolge. Der Anspruch an die künftige Software klang zunächst relativ einfach:

– Ein Endanwender kann mit einem für Laien einfach zu bedienenden WYSIWYG-Editor eigene Berichtsvorlagen generieren.
– Die betriebswirtschaftliche Anwendung ruft zur Laufzeit Vorlagen auf und wandelt sie mit einem Rohdaten-Strom in Bildschirmansichten und Ausdrucke.
– Eingangsdatenstrom und die Druckvorlagen entsprechen einem Standardformat, um einen späteren Tausch einzelner Komponenten sowie die Interoperabilität mit Drittsystemen zu gewährleisten.

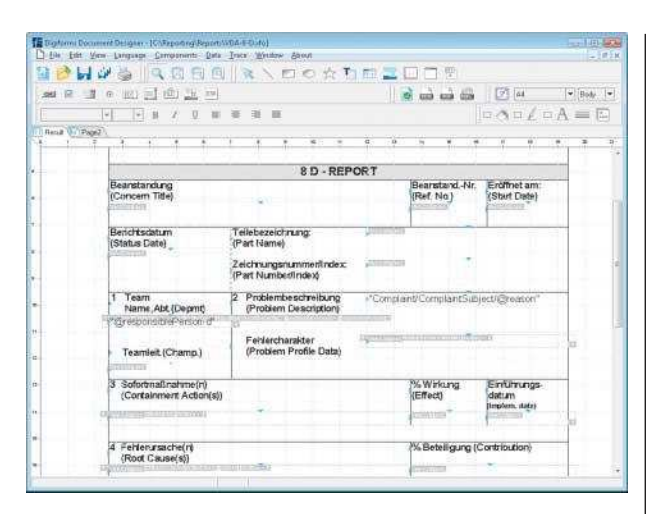
Allerdings schränkten diese Kriterien die Auswahl der infrage kommenden Produkte stark ein.

Standards, wo immer möglich

Nach eingehender Recherche fiel die Entscheidung für XML als Format für die Inhaltsdaten, kodiert in UTF-8. Dies erleichtert die Bereitstellung der eigentlichen Daten durch die betriebswirtschaftliche Anwendung ungemein, da die verwendete Java-Plattform XML-Syntax und -Kodierung von Haus aus unterstützt, eine aufwendige und fehleranfällige Eigenentwicklung des Datenexports deshalb weitgehend entfallen konnte. Umlaute und andere Sonderzeichen zu verarbeiten, wie sie im internationalen Geschäftsverkehr zunehmend eine Rolle spielen, war mit der alten Software nicht machbar; das ist mit UTF-8 ebenfalls passé.

Statische Bilder wie JPGs für Logos et cetera sollten als Referenz im Datenstrom vorkommen, während aus dem Inhalt berechnete Informationen, beispielsweise Balkendiagramme, nicht die Anwendung selbst, sondern ein externer Renderer, sozusagen on the fly, erstellen sollte. Seine Aufgabe war es, aus den XML-Daten anhand von zuvor gestalteten Berichtsvorlagen eine druckbare Zieldatei in einem Standardformat, etwa PDF, zu erzeugen. Das ist mit dem Datenformat XML/UTF-8 gegeben. Mehrfach vorhandene Elemente, beispielsweise ein wiederkehrendes Logo, müssen im Datenstrom nicht zwingend immer wieder auftauchen, sondern man kann sie dank XML einmal definieren und später mehrfach referenzieren. Das verkleinert den zu verarbeitenden Datenstrom und fördert die Performance.

Durch die WYSIWYG-Arbeitsweise erhält der Anwender schon beim Erstellen der Vorlage einen lebendigen Eindruck des späteren Aussehens (Abb. 1).





Eine in XSLT geschriebene Makro-Bibliothek hilft, aufwendige Vektorgrafiken on the fly zu erzeugen (Abb. 2).

Für die Berichtsvorlagen wünschten sich die Autoren ebenfalls XML, in Gestalt von XSL (Extensible Stylesheet Language). Die Sprache erfüllt mit XSLT (XSL Transformations) für die Transformation und XSL-FO (XSL Formatting Objects) für das Layout professionelle Ansprüche. Hinter der Entscheidung für XSL stand der Wunsch, sowohl dem Endanwender die freie Wahl des Bearbeitungswerkzeugs als auch den Programmierern die freie Wahl der Rendering-Engine zu lassen. Das Erzwingen einer bestimmten Produktkombination sollte auf jeden Fall vermieden werden – hauptsächlich aufgrund schlechter Erfahrungen.

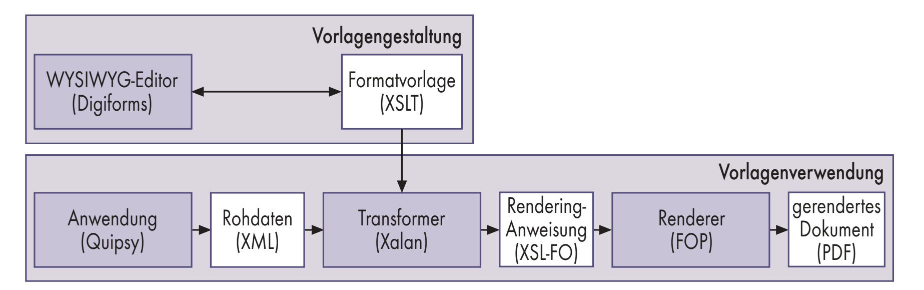
Jeder kennt es, keiner kann es

Zum Zeitpunkt der Recherche (Anfang 2006) waren im Bereich XML-basierter Reporting-Werkzeuge unter anderem bekannte Produkte: Stylus Studio, Xultation Designer, Antenna House Designer, Syntax Serna, Intelliview, XFDesigner, XSLfast sowie Altova Stylevision. Bei genauerer Betrachtung zeigte sich, dass sie sich nur bedingt für den gewünschten Anwendungszweck eigneten. Entweder waren sie zu komplex, was die Kenntnisse der Mehrzahl der Anwender überstiegen hätte, oder es fehlten echte WYSIWYG-Fähigkeiten.

Grund hierfür ist, dass die Hersteller eher Programmierer und weniger „unbedarfte“ Anwender im Blick haben. Ebenso erfüllte nicht jedes Werkzeug den Wunsch, dass Druckvorlagen und Datenstrom auf freien Standards aufsetzen sollten. Viele Produkte können zwar XML verarbeiten, speichern Druckvorlagen jedoch in einem proprietären Format. Ein Austausch von Druckvorlagen zwischen verschiedenen Mitarbeitern mit unterschiedlichen Gestaltungswerkzeugen wäre somit unmöglich, da nicht jeder Hersteller eine Anleitung seines XSD-Schemas beilegt, was für eine Transformation als einzigen Ausweg nötig wäre.

Zu guter Letzt erzwangen eine ganze Reihe von Werkzeugen bestimmte, wiederum proprietäre Rendering-Produkte, wodurch das Kriterium der freien Austauschbarkeit der Rendering-Engine nicht mehr erfüllt war. Überraschend war zudem, dass die Hersteller überwiegend zwar mit den Worten XML oder sogar XSL-FO werben, damit aber keineswegs meinen, dass die Berichtsvorlage selbst in diesem offenen Standard vorliegt. Einige Produkte benutzen XSL-FO nur intern, andere eine proprietäre Formatierungssprache zur Ansteuerung des hauseigenen Renderers (der kostenpflichtig ist).

Unter dem viel zitierten Strich blieb lediglich ein einziges Produkt, das alle genannten Kriterien erfüllte: Der Xul-



Die Prozesskette beruht auf offenen Standards und freien Werkzeugen (Abb. 3).

tation Designer des norwegischen Softwarehauses Metafocus AS, das dieses Produkt inzwischen unter dem geänderten Namen Digiforms Designer vertreibt. Die Produktbeschreibung deckte sich vollständig mit der Liste der geforderten Standards. Die Frage war nur, ob dies in der Praxis zutrifft.

Ehrenrettung aus Norwegen

Version 3.0 des Digiforms Designer ist in erster Linie ein vollwertiges WYSIWYG-Werkzeug zur Erstellung von Vorlagen jeglicher Art, wobei die zu verarbeitenden Eingangsdaten in einem beliebigen XML-Schema vorliegen müssen und das Format der Druckvorlagen den Standards XSLT 1.0, XSL-FO 1.0 sowie XPath 1.0 entspricht. Intern benutzt das Tool Apache FOP 0.20.5 zur PDF-Voransicht, ist zur Laufzeit jedoch keineswegs auf diesen speziellen Renderer angewiesen, da keinerlei proprietäre Erweiterungen zum Einsatz kommen.

Anwendern dürfte als Erstes auffallen, dass die Benutzung stark an ein Malprogramm erinnert: Sie können ohne Vorkenntnisse innerhalb weniger Minuten einen einfachen Bericht mit Tabellen, Textfeldern et cetera gestalten. Ein besonderes Highlight stellt der sogenannte Trace-Mode dar: Ein eingescanntes Formular stellt Digiforms Designer beim Bearbeiten als Hintergrundgrafik dar. Mit einem Klick in die Grafik erkennt der Designer Position und Größe von Datenfeldern im Scan automatisch und fügt entsprechende Eingabefelder in die Druckvorlage ein. Die Umsetzung von papiernem Berichtswesen auf elektronische Berichte ist dadurch ein Kinderspiel. Im Test hat das reibungslos funktioniert.

Der eingebaute XML-Browser ermöglicht eine XPath-Adressübernahme bestimmter XML-Knoten per Mausklick in das gewünschte Berichtsfeld, sodass keine tiefgehenden XPath-Kenntnisse nötig sind. Man klickt einfach auf die Baumdarstellung der Daten und zieht die Information an die gewünschte Stelle in der WYSIWYG-Ansicht der Vorlage. Darüber hinaus kann man sämtliche in XPath 1.0 definierten Funktionen benutzen, sofern man sie kennt. Hierzu ist jedoch das manuelle Schreiben von XPath-Ausdrücken innerhalb des Eigenschaften-Dialogs des Feldes notwendig, was angesichts der Einfachheit von XPath jedoch keinen unangemessenen Lernaufwand nach sich zieht. Darüber hinausgehend stellt das Produkt viele weitere Features zur Verfügung, die jedoch den Rahmen dieses Artikels sprengen würden.

XML rein, SVG raus

Üblicherweise gestaltet sich der Einstieg in die beschriebene Prozesskette etwa so, dass der Anwender per Maus anhand der XML-Struktur ein meist tabellenlastiges Layout gestaltet. Um aber zu einem wirklich anspruchsvollen Druckergebnis zu gelangen, kommt man sicherlich in der Mehrzahl der Anwendungsfälle nicht um das dynamische Generieren von Vektorgrafiken herum, beispielsweise um Balkendiagramme zu erzeugen. Zwar bietet Digiforms Designer hierzu vorgefertigte, rudimentäre Unterstützung der Scalable Vector Graphics (SVG) an – aus XML-Daten generiert er zur Laufzeit eine SVG-Grafik –, jedoch dürfte sich der professionelle Anwender nicht mit diesen Ergebnissen zufriedengeben. Das Produkt ist daher in jeglicher Richtung offen, das heißt, man kann beliebige, in XSLT geschriebene Template-Bibliotheken einbinden und von jedem Feld des Berichts aus aufrufen. Beispielsweise könnte die bekannte Bibliothek XSLTSL zum Einsatz kommen (siehe „Onlinequellen“).

Abbildung 2 zeigt eine Sicht, die die Autoren mit XSLT-Makros in kurzer Zeit erstellt haben. Unter anderem entstand in der Vorbereitung zu diesem Artikel eine Bibliothek mit komplexen mathematischen Funktionen und dynamischen SVG-Diagrammen. Leider werden solche Makros erst zur Laufzeit ausgeführt, sodass in der WYSIWYG-Ansicht lediglich Platzhalter zu sehen sind.

Technisch gesehen läuft die Prozesskette wie in Abbildung 3 dargestellt ab: Die Anwendung übergibt einen XML/UTF-8-Strom mit den Rohdaten an einen beliebigen XSLT-Prozessor. Der Prozessor wandelt unter Nutzung der in XSL (XSLT und XSL-FO) definierten Vorlage und eventuell weiteren, von dieser referenzierten XSLT-Bibliotheken und statischen JPG- oder PNG-Bildern den Datenstrom in ein statisches XSL-FO-Dokument. Hierbei kann die Anwendung eingebettete SVG-Grafiken aus den Daten errechnen.

Da das von den Autoren entwickelte Anwendungssystem in Java programmiert war, entfiel eine Recherche zu alternativen Prozessoren, da die Java Runtime Engine schon einen XSLT 1.0 kompatiblen Prozessor mitbringt. Die Java-VM erlaubt es jedoch, den Prozessor auszutauschen, um beispielsweise einen besonders schnellen zu verwenden. Dementsprechend hat der Anwender die freie Wahl aus einer großen Menge an Produkten.

Per Pipe – ohne Zwischenspeicherung auf der Festplatte – reicht der Designer das XSL-FO-Dokument sodann an einen nachgeschalteten Renderer weiter, der daraus das gewünschte Zielformat erstellt. Durch die offenen Schnittstellen ist es einfach, nicht nur den Vorlagen-Editor und den XSLT-Prozessor zu tauschen, sondern außerdem den XSL-FO-Renderer. Je nach Aufgabe kann man in verschiedene Zielrichtungen optimieren (Ablaufgeschwindigkeit, Speicherverbrauch, zusätzliche Features oder Zielformat).

Als erste Wahl für eine Rendering-Engine kam Apaches FOP ins Spiel, der Default-Renderer des Digiforms Designer. Wie sich herausstellte, arbeitet FOP zwar bei Weitem nicht vollständig fehlerfrei und benötigt viel Arbeitsspeicher, dennoch ist die Software schon in

Onlinequellen

Digiforms Designer	www.metafocus.no/en/
FOP	xmlgraphics.apache.org/fop/
XSLT Standard Library	xsltsl.sourceforge.net/

vielen anderen Projekten erfolgreich im Einsatz und liefert mehr als akzeptable Ergebnisse. Da alle benötigten Funktionen erfüllt waren, erübrigte sich die Evaluierung weiterer Engines.

Fazit

Sieht man vom WYSIWYG-Designer ab, sind für ein professionelles Reporting keine proprietären Formate oder kommerziellen Werkzeuge notwendig. Es ist bedauerlich, dass es anscheinend nur ein einziges Hilfsmittel auf dem Markt gibt, das seine Dateivorlagen als standardkonforme XSL-Dateien ablegt. Doch immerhin ist es relativ günstig und erfüllt alle gestellten Anforderungen.

Entwicklungspotenzial gibt es in zwei Richtungen. Zum einen ist die FOP-Engine relativ langsam und verbraucht viel Hauptspeicher. Je nach Druckvolumen könnte der Wechsel auf ein alternatives Produkt Vorteile mit sich bringen. Nach Beendigung der Arbeit an diesem Artikel erschien ein neues Release von FOP, die schneller arbeitet und weniger RAM benötigt.

Wer komplexe Berichte benötigt, mit vielen Berechnungen und dynamischen Elementen, könnte zum anderen XSL 2.0 sinnvoll finden, das das W3C nach Beendigung des Projekts zum Standard erhoben hat. Jedoch unterstützen diese Version momentan nur die wenigsten Transformer/Renderer, was sich vermutlich jedoch bessern dürfte.

Sollen ausschließlich allgemein akzeptierte Standards zum Einsatz kommen, stellt die gefundene Kombination einen günstigen Umsetzungsweg dar. Es ist zwar noch Verbesserungspotenzial vorhanden, jedoch ist mit FOP 1.0 sowie XSL 2.0 Abhilfe in Sicht. (hb)

MARKUS KARG

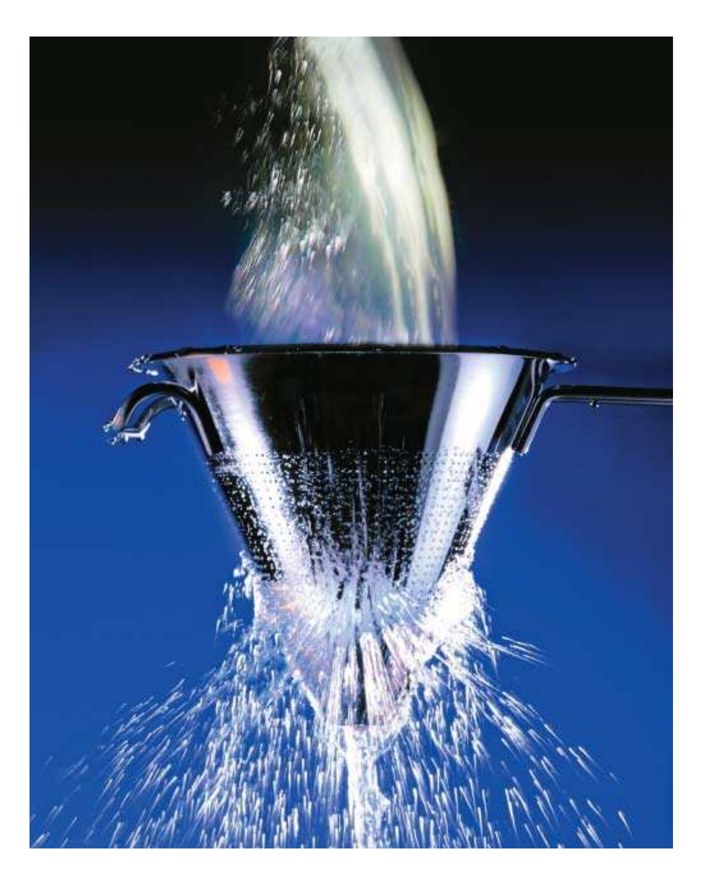
ist staatlich geprüfter Informatiker und verantwortet Implementierung & Design bei der Quipsy Quality GmbH & Co. KG in Pforzheim.

SEBASTIAN KREBS

ist IT-Fachinformatiker in der Anwendungsentwicklung, als Quality Engineer bei der Uniserv GmbH in Pforzheim tätig und studiert Wirtschaftsinformatik.







VoIP-Sicherheit versus Sprachqualität

Sprachbarriere

Peter Backs, Norbert Pohlmann, Claas Rettinghausen

Kritik an Voice over IP bezieht sich meist auf zwei Aspekte: die mangelnde Sprachverständlichkeit und das Fehlen eines Abhörschutzes. *iX* geht der Frage nach, ob und wie sich beide Forderungen erfüllen lassen.

Oft berücksichtigen Entscheider bei der Wahl von VoIP-Lösungen nur die potenzielle Kostenersparnis sowie die flexible und einfache Handhabung, vernachlässigen aber einen anderen wesentlichen Aspekt: die Sicherheit. Die Autoren haben im Rahmen einer Forschungsreihe am Institut für Internet-Sicherheit der FH Gelsenkirchen untersucht, inwieweit unterschiedliche Ansätze helfen, Sicherheitslücken effektiv und einfach zu schließen, und wie stark sie die Benutzung von VoIP beeinflussen.

Voice over IP kapselt Sprachdaten in IP-Pakete und versendet sie über das Internet oder LAN. Üblicherweise kommt dabei das User Datagram Protocol (UDP) zum Einsatz, das im Gegensatz zu TCP keine Liefergarantie gibt. Es eignet sich jedoch besser für Echtzeitkommunikation: Das Neuanfordern verlorener Pakete, wie es TCP durchführt, führt zu Verzögerungen, die die Sprachqualität verschlechtern können. Allerdings genügt UDP allein nicht für eine isochrone Audio- oder Video-Übertragung. Dafür zeichnet das auf UDP aufsetzende Realtime Transport Protocol (RTP) verantwortlich. Das dazugehörige RTP Control Protocol (RTCP) misst während des Telefonats periodisch die Übertragungsqualität des Transportnetzes. Beide sind in RFC 3550 spezifiziert (siehe Kasten „Onlinequellen“).

Zur Anrufsteuerung verwendet man meist das Session Initiation Protocol (SIP, RFC 3261). Es signalisiert dem anderen Teilnehmer, dass ein Gespräch stattfinden soll, handelt die Kommunikationsparameter aus – etwa UDP-Ports und die zu verwendende Sprachkodierung – und beendet die Verbindung wieder, sobald ein Teilnehmer den Hörer auflegt.

Wartezeiten unerwünscht

Einfluss auf die Sprachqualität einer VoIP-Verbindung nimmt unter anderem der verwendete Codec. Er wandelt das analoge Sprachsignal in ein digitales und umgekehrt. Steht nur eine geringe Übertragungskapazität zur Verfügung – etwa im WAN –, kann er die Sprachdaten zusätzlich komprimieren. Wichtiger ist jedoch, dass sich das Signal mit minimaler Verzögerung kodieren und dekodieren lässt. Tabelle 1 führt die bei der Untersuchung berücksichtigten Codecs auf.

Auch die Eigenschaften des Netzes – gemeinhin unter dem Schlagwort „Quality of Service“ (QoS) zusammengefasst – beeinflussen die Qualität der Sprachübertragung. Für gute Verständlichkeit sind drei Kriterien zu erfüllen:

– Die benötigte Übertragungskapazität muss während des gesamten Gesprächs zur Verfügung stehen.
– Paketverluste (Packet Loss) müssen verhindert oder durch den Codec ausgeglichen werden.
– Pakete müssen rechtzeitig und regelmäßig beim Empfänger eintreffen (Delay, Jitter).

Je nach Entfernung der Endgeräte und Anzahl der Router auf dem Übertragungsweg kann die Verzögerung (Delay) stark schwanken. Die Signallaufzeit (Propagation Delay) – die Zeit, die ein Signal dafür benötigt, eine Leitung zu durchqueren – ist proportional zur Entfernung, genauer gesagt zur Leitungslänge. Hinzu kommt die Vermittlungsverzögerung (Switching Delay). Netzkoppelelemente wie Router oder Switches müssen

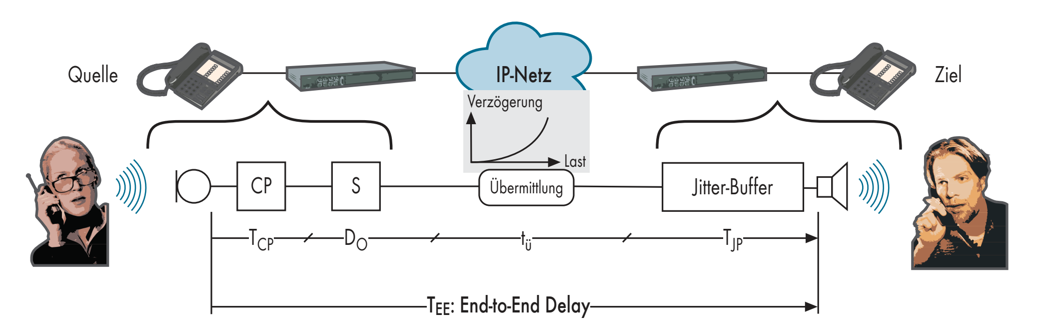
Sprach-Codecs

Codec	Delay (ms)	Bitrate (kBit/s)	MOS
G.711 µ-Law	10	64	4,1-4,5
G.711 A-Law	10	64	4,1-4,5
G.726	1	32	3,85-4,2
G.723.1	30	6,3	3,9
G.729a	10	8	3,9
GSM	20	13,2	3,75

in der Regel warten, bis alle Bits eines Pakets eingetroffen sind. Anschließend wählen sie eine Route zum Empfänger und serialisieren die Bits wieder (Store-and-Forward). Die Warteschlangen eines Routers verzögern die Verarbeitung zusätzlich (Queueing Delay). Muss ein Rechner aufgrund des Zugriffsverfahrens des Netzes – etwa CSMA/CD bei Ethernet – warten, bis er Daten senden darf, spricht man von Zugriffsverzögerung (Access Delay). Sie ist jedoch in der Regel vernachlässigbar.

Der maximale Durchsatz ergibt sich aus der verwendeten Hardware, wobei das schwächste Glied die Kapazität einer Übertragungsstrecke bestimmt. Theoretisch sind Verzögerung und Durchsatz voneinander unabhängig. Messungen zeigen jedoch, dass mit steigendem Verkehrsaufkommen auch die Verzögerung steigt.

Jitter steht bei VoIP für Schwankungen der Verzögerungszeit (Delay Jitter), die ihrerseits die Sprachqualität herabsetzen. Üblicherweise enthalten VoIP-Endgeräte deshalb einen Jitter-Puffer, der die Unregelmäßigkeiten ausgleicht. Er erhöht jedoch wiederum die Gesamtverzögerung (siehe Abbildung 1).



Lange Reise: Netze, VPN-Router und Endgeräte tragen zur Verzögerung des Sprachsignals bei (Abb. 1).

Das Ohr als Messgerät

Leider liefern die Zahlen keine direkte Aussage, ob ein VoIP-Gespräch verständlich ist oder nicht. Darum wurden Verfahren entwickelt, die die Verbindungsqualität durch eine einzige Zahl bewerten:

– Mean Opinion Score (MOS) ist der am häufigsten zu findende Wert zur Qualitätsbeschreibung. Man ermittelt ihn, indem man eine repräsentative Auswahl von Testpersonen Sprachproben auf einer Skala von 1 bis 5 bewerten lässt (siehe Tabelle 2). Dabei steht der Wert 5 für optimale Sprachqualität; ISDN-Verbindungen erreichen einen MOS von etwa 4,5, analoge Festnetzverbindungen ungefähr 3,5. Andere Verfahren, die ohne die subjektive Bewertung durch Testpersonen auskommen, können den MOS rechnerisch herleiten.

– Sprachmusterorientierte Verfahren senden ein definiertes Sprachmuster über ein Netz und vergleichen das an der Gegenstelle eintreffende Signal mit dem ursprünglichen. Das für VoIP wichtigste Verfahren Perceptual Evaluation of Speech Quality (PESQ) hat die ITU-T in der Empfehlung P.862 ratifiziert. Der Vorgänger PSQM (Perceptual Speech Quality Measurement) berücksichtigte nur den Einfluss des Codecs auf die Sprachqualität, PESQ lässt darüber hinaus die QoS-Parameter in die Bewertung einfließen. Es funktioniert allerdings bei „schlechten“ Netzen mit hohem Delay oder Packet Loss nicht zuverlässig. Als Ergebnis liefert PESQ unter anderem den hergeleiteten MOS.

– Netzbasierte Verfahren bewerten die Verbindungsqualität passiv, ohne das Einspielen spezieller Sprachmuster. Das häufig verwendete E-Modell produziert anhand der gemessenen und erwarteten QoS-Parameter sowie des verwendeten Sprachcodecs den sogenannten R-Faktor, der die Qualität der Sprachübertragung angibt. Er liegt zwischen 0 und 100, wobei 100 optimale Sprachqualität bedeutet; 94 entspricht ISDN-Qualität. Der R-Faktor lässt sich ebenfalls in den entsprechenden MOS umrechnen.

Nicht für aller Ohren

Telefonie ist vor E-Mail und Post nach wie vor das wichtigste Kommunikationsmedium der heutigen Gesellschaft. Geradezu selbstverständlich verlassen sich Nutzer von analogen oder ISDN-Telefonen auf die Sicherheit der Telefonnetze, deren Schutz ausschließlich von den Beschränkungen des physischen Zugangs zur Telefonleitung abhängt.

Bei VoIP muss der Angreifer ebenfalls Zugang zu den Systemen oder Übertragungsmedien haben, die die VoIP-Telefonate übermitteln. Durch einfache Spoofing-Angriffe und die für den Benutzer nicht vorhersehbaren Routingwege der IP-Pakete erhöht sich die Zahl der potenziellen Angreifer im Vergleich zur herkömmlichen Telefonie jedoch erheblich. Zudem ist ungesichertes VoIP mit einem normalen PC und frei erhältlicher Software kompromittierbar, während man für das Abhören von ISDN-Gesprächen zumindest spezielle – obgleich nicht komplizierte – Hardware benötigt. Wer die Sicherheit eines VoIP-Gesprächs gewährleisten will, muss daher zusätzliche Maßnahmen ergreifen.

Sicherungsmechanismen können sowohl VoIP-spezifisch als auch allgemeiner Natur sein. Zu Letzteren zählen Virtual Private Networks

iX-TRACT

- VoIP-Verbindungen lassen sich mit protokollspezifischen oder allgemeinen Verfahren sichern.
- Beide Ansätze erhöhen die zu übertragende Datenmenge, wirken sich jedoch nur unwesentlich auf QoS-Parameter wie die Verzögerung aus.
- In langsamen Netzen empfiehlt es sich, VoIP-spezifische Sicherheitsmaßnahmen wie Secure RTP (SRTP) einzusetzen, da sie weniger Overhead erzeugen.

Die MOS-Skala (Mean Opinion Score)

MOS	Rating	Bedeutung
5	excellent	keinerlei Anstrengung zum Verständnis der Sprache notwendig; totale Entspannung möglich
4	good	keine Anstrengung, aber Aufmerksamkeit notwendig
3	fair	leichte, moderate Anstrengung nötig
2	poor	merkbare, deutliche Anstrengung nötig
1	bad	keine Verständigung möglich

(VPN). Sie können den gesamten Verkehr zwischen zwei oder mehreren Netzen absichern.

Da der Verschlüsselungskanal (Security Association, kurz SA) bei einem VPN meist permanent besteht, muss man die verwendeten Schlüssel regelmäßig ändern. Das sogenannte Re-Keying kann während eines Gesprächs Einfluss auf die Qualität der Verbindung und damit auf die VoIP-Sprachqualität haben, wenn der Aufbau einer neuen SA erst mit dem Ablaufen der alten stattfindet. Daher sollte die VPN-Lösung in der Lage sein, neue SAs rechtzeitig vor dem Ablaufen der momentan verwendeten zu erzeugen.

Keine Infrastruktur für Public Keys

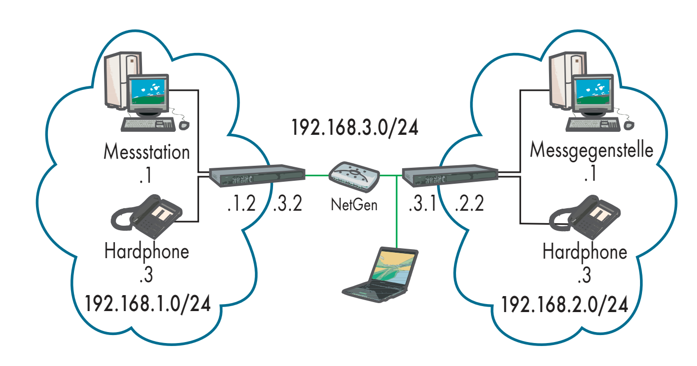
Darüber hinaus hat eine generische Lösung wie ein VPN den Nachteil, dass die Sicherung erst an der Grenze des lokalen Netzes beginnt beziehungsweise endet. Das LAN transportiert alle Sprachdaten unverschlüsselt, ein Angreifer kann sie daher leicht lesen. Außerdem sind organisationsübergreifende VPNs – etwa eine Kopplung unterschiedlicher Firmennetze – nur mit erheblichem Aufwand realisierbar, weshalb eine flächendeckende VoIP-Absicherung oft scheitert. In erster Linie eignet sich der VPN-Ansatz daher für den internen VoIP-Verkehr einer Organisation.

VoIP-spezifische Sicherheitsmaßnahmen erweitern die existierenden VoIP-Protokolle. Üblicherweise überträgt man SIP-Daten per SSL/TLS gesichert (SIPS) von einem Hop zum nächsten und verwendet Secure RTP (SRTP, RFC 3711) zur Verschlüsselung des Medienstroms zwischen den Teilnehmern (End-to-end).

Von entscheidender Bedeutung ist dabei die Vertrauenskette zwischen den an der Signalisierung beteiligten Intermediären, etwa den SIP-Gateways der jeweiligen Provider. Die Teilnehmer tauschen die für SRTP verwendeten Schlüssel im Klartext innerhalb der SIP-Signalisierungsnachrichten aus. Dadurch kommen die Intermediäre in den Besitz der Schlüssel, und es besteht die Gefahr eines Man-in-the-middle-Angriffs (MITM Attack).

Des Weiteren ist eine organisationsübergreifende Public-Key-Infrastruktur (PKI) oder eine andere Infrastruktur für kryptografische Schlüssel Voraussetzung, um Kommunikationspartner zu authentifizieren. Angesichts der Tatsache, dass sich eine weitflächige PKI etwa für den E-Mail-Dienst bislang nicht durchsetzen konnte, bleibt jedoch zweifelhaft, ob sich verbreitetes sicheres Telefonieren mit den etablierten VoIP-Standards durchsetzen wird.

Um den organisatorischen Aufwand zu umgehen, hat PGP-Erfinder Philip R. Zimmermann ein Protokoll entwickelt, das ohne PKI auskommt: ZRTP führt eine ungesicherte Diffie-Hellman-Schlüsselaushandlung durch und baut anhand der daraus abgeleiteten Schlüssel einen gesicherten SRTP-Kanal auf. Um die konzeptionell bedingte Anfälligkeit des Verfahrens gegen Man-in-the-middle-Angriffe zu kompensieren, stellt ZRTP einen Hash-Wert der öffentlichen Diffie-Hellman-Keys bereit, den die Gesprächspartner mündlich („Inband“) vergleichen und sich dadurch authentifizieren können. Nachteilig bei dem Verfahren ist, dass die Authentifizierung durch den Menschen erfolgt, was naturgemäß nie völlig sicher ist. Außerdem lassen sich fremde Stimmen – im Geschäftsumfeld die Regel – prinzipiell nicht authentifizieren.



Messaufbau zur Untersuchung des Einflusses von VPN-Tunneln auf die Quality of Service (QoS) (Abb. 2).

Sicher und trotzdem verständlich

Den Einfluss der Sicherungsmaßnahmen auf die Sprachqualität haben die Autoren im Labor untersucht. Alle Messungen fanden in einem isolierten LAN statt, um Störquellen im Netzwerk auszuschließen und unverfälschte Messergebnisse zu garantieren. Der Testaufbau bestand aus drei unterschiedlichen Subnetzen: den Sender- und Empfänger-Netzen *192.168.1.0* und *192.168.2.0* sowie dem Transportnetz *192.168.3.0*. Die Subnetze mit den VoIP-Komponenten sind durch Security Gateways gekoppelt (siehe Abbildung 3).

Als VPN-Gateways kamen die frei verfügbare IPsec-Implementierung OpenSWAN und das ebenfalls freie OpenVPN (SSL/TLS) zum Einsatz. Ein Netz mit gewöhnlichen Routern anstelle der VPN-Gateways diente als Referenz. Die Messungen wurden mit einer Beta-Version des QoS-Messsystems NetGage, entwickelt vom Projekt QoSSIP der FH Köln, und der VoIP Test Suite von ITD Informationstechnologie durchgeführt. Die Bridge-Software NetGen – ebenfalls eine Entwicklung des QoSSIP-Projekts – simulierte zwischen den Gateways ein reales Netz mit einstellbarem Delay, Jitter und Packet Loss. Mit dem Netzbenchmark Iperf erhöhten die Tester schrittweise die Last im Netz.

Sowohl mit NetGage als auch mit der VoIP Test Suite ließ sich der Einfluss der VPN-Tunnel auf Jitter und Packet Loss messen und ergaben eine zusätzliche Ver-

Onlinequellen

Institut für Internet-Sicherheit der FH Gelsenkirchen	www.internet-sicherheit.de
RFC 3550 – RTP: A Transport Protocol for Real-Time Applications	tools.ietf.org/html/rfc3550
RFC 3261 – SIP: Session Initiation Protocol	tools.ietf.org/html/rfc3261
RFC 3711 – The Secure Real-time Transport Protocol (SRTP)	tools.ietf.org/html/rfc3711
ZRTP: Media Path Key Agreement for Secure RTP	zfoneproject.com/docs/ietf/draft-zimmermann-avt-zrtp-06x.html
OpenSWAN	www.openswan.org
OpenVPN	openvpn.net
QoSSIP-Projekt	www.qossip.de/index.php?catid=25
ITD VoIP Test Suite	www.trafficlyser.de/hp/itd/front_content.php?idcat=306
Iperf	dast.nlanr.net/projects/Iperf/

zögerung von ein bis zwei Millisekunden, die für die Sprachverständlichkeit nahezu unerheblich ist.

Beide VPN-Gateway-Implementierungen können die übertragenen Daten zusätzlich komprimieren. Verwendet man den PCM-Codec G.711, gleicht die Kompression den durch die Gateways entstehenden Overhead aus. Kommt ein komprimierender Codec zum Einsatz, bleibt die zusätzliche Kompression im Gateway ohne Wirkung. In beiden Fällen erhöht sich die Verzögerung um weniger als eine Millisekunde. Da die Gateways bei aktivierter Kompression mehr Arbeit leisten müssen, ist allerdings zu erwarten, dass der Gesamtdurchsatz sinkt.

Beim VoIP-spezifischen Ansatz ließen sich mit der eingesetzten Software keine detaillierten Messungen durchführen – sie beherrscht die verwendeten Sicherungsprotokolle noch nicht. Allein den Datendurchsatz beziehungsweise die Bitrate kann man zuverlässig messen. Daraus ergibt sich ein Overhead von rund rund 10 %, bei Verwendung von SRTP sowie den Codecs G.723.1 und G.729a. Die VPN-Gateways verursachen in derselben Situation mit oder ohne Kompression einen Overhead zwischen 75 und 90 % relativ zu einer ungesicherten Verbindung. Allerdings können mehrere Parameter die Messungen beeinflussen:

– Paketierung der Sprachsegmente: Überträgt man mehrere Sprachsegmente pro IP-Paket, verringert sich der Protokoll-Overhead. Die Verzögerung nimmt jedoch zu.

– Codec-Bitrate: Die Codecs unterscheiden sich hinsichtlich der benötigten Übertragungskapazität und der Sprachqualität voneinander.

– Codec-Segmentgröße: Abhängig von der Segmentgröße übertragen Codecs mehr oder weniger Pakete auf einmal, was den Protokoll-Overhead beeinflusst.

– Blockgröße der verwendeten Verschlüsselung: Die verwendeten Algorithmen verschlüsseln Daten blockweise. Stehen nicht genug Daten zur Verfügung, müssen sie Null-Bytes als „Füller“ einfügen.

Fazit

Die untersuchten Sicherheitsmaßnahmen wirken sich vorrangig auf die benötigte Übertragungskapazität aus, nicht jedoch auf Delay, Jitter oder Packet Loss. Abhängig von den Einstellungen der VoIP-Software und der Security-Gateways kann sich die Größe der VoIP-Pakete mehr als verdoppeln. Anwendern mit langsamer Internetanbindung sowie Unternehmen mit vielen VoIP-Nutzern kann dies erhebliche Schwierigkeiten bereiten. Durch geeignete Einstellungen der VoIP- und Verschlüsselungssoftware lässt sich jedoch die Bitrate beeinflussen. Ist die zur Verfügung stehende Übertragungskapazität gering, sollte man jedoch das VoIP-spezifische SRTP einem VPN-Tunnel vorziehen. (mr)

PETER BACKS

ist IT-Consultant/Developer bei der Sirrix AG in Saarbrücken.

PROF. DR. NORBERT POHLMANN

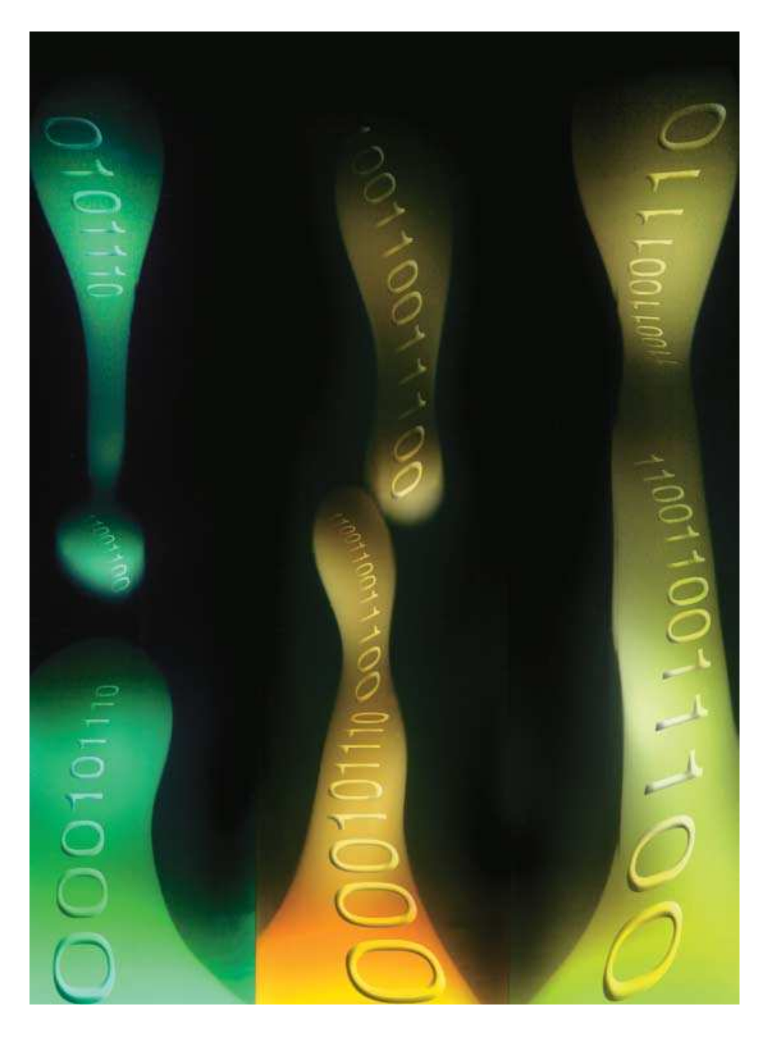
ist Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie Leiter des Instituts für Internet-Sicherheit – if(is) an der Fachhochschule Gelsenkirchen.

CLAAS RETTINGHAUSEN

ist VoIP System Architekt bei der Carpo Deutschland GmbH in Ratingen.







Parallele Anwendungen entwickeln mit Erlang/OTP

Neben- und Miteinander

Frank Müller

Nicht viele funktionale Programmiersprachen haben den Weg aus der akademischen Nische heraus geschafft. Erlang ist eine davon. Ein kompakter Code, in dem Nebenläufigkeit und Verteilung eine entscheidende Rolle spielen, prädestinieren die Sprache für skalierbare und hochverfügbare Anwendungen.

Jahrelang steigerte sich die Performanz von Rechnersystemen durch die Erhöhung des Prozessortakts. Dieser Weg hat jedoch seine Grenzen, beispielsweise wegen thermischer Schwierigkeiten. Eine Alternative ist die parallele Verarbeitung mit multiplen Ablaufpfaden auf der CPU durch mehrfache Prozessorkerne oder Multiprozessorsysteme. So sind Notebooks heute mit Dual-Core-Prozessoren ausgestattet, Hochleistungs-PCs mit bis zu acht Kernen und Server mit einer großen Anzahl von CPUs. Allerdings ist es nicht eben trivial, Aufgabenstellungen zu parallelisieren geschweige denn, dies in Code zu gießen. Eine Plattform, die dem Entwickler bei verteilten und parallelen Anwendungen entgegenkommt, ist Erlang/OTP.

Immer mehr Programmierer sehen sich vor die Aufgabe gestellt, solche Systeme zu entwickeln, sodass der Name Erlang in letzter Zeit mehr und mehr auftaucht. Die Geschichte der Sprache sowie der dazugehörigen Plattform beginnt jedoch schon viel früher. Der Grundstein wurde bereits 1984 gelegt, als Joe Armstrong, Göran Båge, Seved Torstendahl und Mike Williams das Computer Science Laboratory (CSLab) des Telekommunikationsunternehmens Ericsson gründeten. Eine der Aufgaben dieses Teams war die Entwicklung einer Softwareinfrastruktur für Telekommunikationssysteme. Hierzu experimentierten die Forscher mit verschiedenen Formen imperativer, deklarativer, regelbasierter und objektorientierter Sprachen und prüften sie auf ihre Eignung für das Einsatzgebiet der Telefonie.

Anforderungen an die Programmiertechnik waren eine massiv-parallele Verarbeitung sowie die Möglichkeit, asynchrone Nachrichten zwischen den Prozessen zu senden. Weiterhin sollten Updates zur Laufzeit einen unterbrechungsfreien Betrieb gewährleisten. Ein weiterer Anspruch war, Programme mit wenig und elegantem Code realisieren zu können, der sich dicht an der formalen Spezifikation orientiert. Die Motivation hierfür lag in der Erkenntnis, dass die Anzahl fehlerfrei entwickelter Code-Zeilen pro Tag unabhängig von der gewählten Programmiersprache ist. Somit sollte wenig Code pro Funktion zu einer geringen Fehlerträchtigkeit führen.

Einige dieser Eigenschaften waren zu dieser Zeit mit Prolog möglich, sodass Erlang zunächst auf dieser deklarativen Sprache basierte, ergänzt durch Nebenläufigkeit. Allerdings erwies sich im Laufe der Entwicklung das Backtracking von Prolog als ungeeignet, und die Weichen wurden in Richtung funktionaler Programmierung gestellt. Um einen geeigneten Namen für die neue Sprache zu finden, griff das Entwicklerteam auf die Tradition zurück, Programmiersprachen nach Mathematikern zu benennen. Nach Pascal, Euclid und Occam fiel die Wahl auf A.K. Erlang, dessen Formel für Warteschlangenprobleme in der Telefonie zudem einen Bezug zu Herstellern von Telekommunikationstechnik herstellt. Damit steht der Name Erlang entgegen der vielfach vertretenen Meinung nicht für den Begriff Ericsson Language.

Parallel und unterbrechungsfrei

Die während der Entwicklung von Erlang getroffenen Design-Entscheidungen finden sich teils in weiteren zu diesem Zeitpunkt bereits bekannten Sprachen wieder, sind teils jedoch auch einmalig. Letztendlich repräsentiert Erlang einen individuellen Mix für die spezifischen Anforderungen und ist daher eher pragmatisch denn an einer reinen Lehre orientiert.

Eine ihrer signifikanten Eigenschaften ist die Nutzung einer virtuellen Maschine für

Portabilität unabhängig vom Betriebssystem. Ericsson bietet Erlang heute für Solaris, Linux, Windows und VxWorks an, in der Open-Source-Version zusätzlich für Mac OS X und im Quelltext. Nebenläufigkeit sowie Speicherverwaltung inklusive der Garbage Collection sind Aufgabe der VM.

VM sorgt für Plattformunabhängigkeit

Erlang ist dynamisch typisiert und kennt neben Integer- und Fließkommazahlen, Atomen und Bit-Strings noch Referenzen, Prozess- und Portidentifikatoren sowie Funktionsobjekte. Referenzen sind in einer Laufzeitumgebung immer eindeutig, Ports dienen der Kommunikation mit der Außenwelt. Als komplexere Datentypen gibt es Tupel, Listen und Strukturen. Letztere bildet Erlang intern jedoch transparent auf Tupel ab. Strings und Booleans sind keine eigenen Datentypen, sondern werden durch Listen von Integerwerten beziehungsweise die Atome *true* und *false* repräsentiert.

Ein wichtiges Sprachmittel ist die Endrekursion von Funktionen. Sie erlaubt die Implementierung aller Schleifen – auch der unendlichen – als rekursive Funktionen, ohne dass es zu Speicherüberläufen kommt. Auf dieser Basis sind auch die langlaufenden Prozesse möglich, die keinen linearen Durchlauf darstellen. In ihnen wird die Prozessfunktion immer wieder endrekursiv aufgerufen. Mit dem *receive*-Konstrukt greift sie auf die asynchrone Nachrichtenschlange des Prozesses zu und verarbeitet die Nachricht.

Für den Empfang der Nachrichten kommt das in Erlang überall gegenwärtige Pattern Matching zum Einsatz. Es erlaubt die einfache Analyse von Termen für die Zuweisung von Werten zu Variablen. Die letzte wichtige Eigenschaft ist die standardisierte Fehlerbehandlung, die einen aggressiven Programmierstil unterstützt.

Mit der Implementierung dieser Plattform fiel Ende 1987 die Wahl auf Erlang als Software-Basis für eine Telefonanlage. Der Prototyp dieser Anlage wurde 1989 fertiggestellt und erfüllte die in ihn gestellten Erwartungen voll. Im Rahmen einer Evaluierung im Projekt ACS/Dunder haben die Entwickler die Effizienzverbesserung im Design gegenüber der zu der Zeit üblichen Sprache PLEX mit einem Faktor zwischen 9 und 22 bewertet. War die erste Implementierung noch ein Interpreter auf der Basis von Prolog, folgten später ein Compiler sowie eine abstrakte Maschine für die Ausführung. Bis 1992 erreichte Erlang den Status der Produktionsreife und konnte für hardwarenahe Anwendungen mit nahezu Echtzeitanforderungen eingesetzt werden.

iX-TRACT

- Bereits vor über zwanzig Jahren entstanden, rückt Erlang/OTP zunehmend in das Blickfeld von Programmierern, die massiv-parallel arbeitende, verteilte Anwendungen entwickeln müssen.
- Erlang ist eine funktionale Programmiersprache, kann jedoch ihre in Prolog liegenden Wurzeln nicht verleugnen, sodass die Syntax für Einsteiger gewöhnungsbedürftig ist.
- Dennoch erleichtert Erlang durch seine Spracheigenschaften sowie die durch die virtuelle Maschine gegebenen Plattformunabhängigkeit und nicht zuletzt durch die umfangreiche OTP-Bibliothek die Entwicklung verteilter, performanter Systeme erheblich.

Die erste Ebene eines Erlang-Anwendungssystems sind Nodes. Jede gestartete virtuelle Maschine stellt einen solchen Node dar und ist mit weiteren Nodes vernetzbar. Diese können auf dem gleichen System oder weiteren Rechnern im Netz laufen. Allerdings ist es nicht möglich, dass ein Node in mehrere solcher Netze integriert ist. Eine Kommunikation über Netzgrenzen hinweg ließe sich via IP realisieren. Erlang/OTP bringt unter anderem umfangreiche CORBA-Bibliotheken mit, die im Erlang-Sprachgebrauch Module sind. Sie fassen Funktionen zusammen und bilden gleichzeitig einen Namespace. Innerhalb der Module werden die für eine externe Nutzung definierten Funktionen explizit exportiert (Listing 1). Ein Import ist im Gegensatz zu Sprachen wie Java oder C# nicht notwendig, jedoch möglich. Ein Aufruf der Funktionen erfolgt üblicherweise über *modul:funktion (Arg1, Arg2, …)* (Listing 2). Alternativ werden Funktionen explizit importiert und benötigen dann das Modul-Präfix nicht mehr (Listing 3).

Wie in der aus der Objektorientierung bekannten Polymorphie können die innerhalb der Module definierten Funktionen mehrfach in unterschiedlichen Implementierungen vorliegen. Solange die Anzahl der Argumente gleich ist, trennt ein Semikolon die Definitionen. Innerhalb der Funktionen trennen Kommata die Anweisungen sequenziell, und ein Punkt bezeichnet das Ende einer Definition.

Guards ergänzen Pattern Matching

Die Entscheidung darüber, welche Funktionsdefinition eine Anwendung bei einem Aufruf heranzieht, erfolgt über Pattern Matching, teilweise im Zusammenhang mit Guards (siehe unten). Nicht nur die Funktionsauswahl basiert auf Pattern Matching, Muster spielen auch bei *case*-, *receive*- und *try*-Anweisungen sowie beim Match-Operator (=) eine Rolle. Hierbei gleicht der Compiler ein Muster gegen einen Ausdruck ab. Das Muster kann ungebundene Variablen enthalten, die eine Anwendung bei einem passenden Muster setzt (Listing 4). Auf diese Weise extrahiert ein Programm Werte aus Tupeln, liest sie vom Anfang einer Liste oder weist sie direkt zu. So ist es auch zu verstehen, dass es sich bei einem Gleichheitszeichen nicht um eine reine Zuweisung handelt. Im Falle der angesprochenen Funktionsauswahl kommt die zum Tragen, die zum übergebenen Muster passt. Trifft hingegen kein Muster zu, gibt es einen Fehler.

Einfache Muster genügen jedoch nicht immer. Manchmal muss man sicherstellen, dass ein Argument den richtigen Typ hat, manchmal soll er sich auch in einem vorgegebenen Wertebereich bewegen. Denkbar wäre beispielsweise eine Buchungsvariante A bei

Listing 1

```
-module(module_a).
-export([hello/2]).
hello(Place, Who) ->
   io:format("Hello ~p, ~p", [place(Place), Who]).
place(world) -> "world";
place(earth) -> "earth";
place(somewhere) -> "somewhere out there";
place(_Any) -> "wherever you are".
```

Module exportieren für die externe Nutzung definierte Funktionen.

Listing 2

```
-module(module_b).
-export([call_hello/1]).
call_hello(Place) ->
    module_a:hello(Place, "Joe").
```

Listing 3

```
-module(module_c).
-export([call_hello/1]).
-import(module_a, [hello/2]).
call_hello(Place) ->
    hello(Place, "Joe").
```

Ein Funktionsaufruf erfolgt entweder über ein Modul-Präfix (Listing 2) oder über eine Import-Anweisung (Listing 3).

Listing 4

```
-module(module_d).
-export([list_max/1]).
list_max([Head|Rest]) ->
    # Check rest against the first element.
    list_max(Rest, Head).
list_max([], ResultSoFar) ->
    # List to test is empty, return result.
    ResultSoFar;
list_max([Head|Rest], ResultSoFar) when Head > ResultSoFar ->
    # This head is the new maximum result.
    list_max(Rest, Head);
list_max([Head|Rest], ResultSoFar)  ->
    # Head is lower or equal, so go on with the rest.
    list_max(Rest, ResultSoFar).
```

Das Muster bestimmt die Wahl der Funktion.

Listing 5

```
-module(module_e).
-export([book/3]).
book(Amount, From, To) when is_float(Amount), Amount < 1000.0 ->
    ...
book(Amount, From, To) when is_float(Amount), Amount > 10000.0 ->
    ...
book(Amount, From, To) when is_float(Amount)  ->
    ...
book(Anything, From, To) ->
    throw(illegal_data_type).
```

Guards ergänzen das Pattern Matching.

Listing 6

```
-module(module_f).
-export([start/1]).
start(InitialState) ->
   register(my_server, spawn(module_f, loop, [InitialState])).
% Process loop.
loop(State) ->
   receive
       {do_this, Arg1, Arg2} ->
           NewState = handle_this(Arg1, Arg2, State),
           loop(NewState);
       {do_that, Arg1} ->
           NewState = handle_that(Arg1, State),
           loop(NewState);
       stop ->
           ok
   end.
% handle_this and handle_that have to return the new state.
...
```

Zustände von Prozessen werden über die Argumente abgebildet.

einem Betrag kleiner 1000 Euro, Variante B bei 1000 bis unter 10 000 Euro und Variante C bei 10 000 Euro und mehr. Hier kommen die Guards zum Einsatz (Listing 5). Bei der Definition der Guards sind Verknüpfungen via „und“ (Komma) sowie „oder“ (Semikolon) möglich. Gemeinsam erlauben das Pattern Matching und Guards die intelligente und flexible Organisation des Codes.

Variablen sind unveränderbar

Erlang ist sequenziell funktional ausgelegt. Jede Funktion liefert das Ergebnis des letzten Ausdrucks zurück. Wie viele funktionale Sprachen verfügt Erlang über Higher Order Functions, die sich bei der Entwicklung von Modulen wie *lists* als hilfreich erweisen. Das *lists*-Modul bietet Funktionen wie *filter, fold, foreach* und *map* zur Anwendung anonymer Funktionen auf Listen. Das Ergebnis sind neue Listen oder im Falle von *fold* das berechnete Ergebnis. Listen selbst lassen sich nicht verändern. Gleiches gilt für Tupel, Records oder beliebige andere Variablen. Hier stutzen Umsteiger in der Regel: Erlang-Variablen lassen sich nach einer initialen Zuweisung nicht mehr modifizieren. Die Motivation hierfür liegt unter anderem in der Vermeidung von Seiteneffekten. So führt in vielen Sprachen die Modifikation von Variablen, die als Referenz an eine Funktion übergeben werden, häufig zu schwer nachvollziehbaren Fehlern. Dies vermeidet Erlang. Gleichzeitig erleichtern Variablen mit einmaliger Zuweisung die Realisierung der wichtigsten Spracheigenschaft neben dem funktionalen Charakter: der Nebenläufigkeit.

Prozesse sind in Erlang leichtgewichtig und unabhängig vom Betriebssystem ausgelegt. Ihre Ausführung erfolgt durch die virtuelle Maschine, sodass sie sich auf unterschiedlichen Plattformen einheitlich verhalten. Gleichzeitig sorgt die VM für die Aufteilung der Prozesse auf die konfigurierten Kerne oder Prozessoren. Der Datenaustausch zwischen den Prozessen erfolgt im Gegensatz zu vielen Thread-Implementierungen nicht im Shared Memory. Vielmehr verfügt jeder Prozess über eine eigene Message Queue, an die weitere Prozesse – auch über Node-Grenzen hinweg – Nachrichten senden können. Mittels *receive* und dem bereits genannten Pattern Matching kann der Empfänger die Nachrichten selektiv auslesen und verarbeiten. Über endrekursive Aufrufe lassen sich so interne Dienste implementieren, die mit einem kleinen Trick auch über einen Status verfügen können (Listing 6). Dieses Verfahren findet sich in einer Vielzahl der mitgelieferten Module wieder.

Die so erzeugten Prozesse kann man entweder anonym starten – in diesem Fall müssen aufrufende Prozesse die Prozess-ID kennen – oder sie mit einem einmaligen Namen registrieren. Dieser lässt sich dann für das Versenden der Nachricht nutzen. Als Operator hierfür fungiert das Ausrufezeichen (*!*) (Listing 7). Allerdings wird es in der Regel in exportierten Komfortfunktionen versteckt, sodass der Entwickler nicht immer auf den ersten Blick entdeckt, dass seine Anwendung asynchron mit einem Prozess kommuniziert. Auch beim Laufzeitverhalten fällt das nicht auf. So können Erlang-Nodes problemlos mehrere 10 000 Prozesse parallel betreiben und dabei je nach Systemlast dennoch Antwortzeiten kleiner als eine Millisekunde liefern. Die effizient arbeitende Garbage Collection trägt hierzu bei.

Wie erwähnt lassen sich mehrere Nodes vernetzen. Eine einfache Authentifizierung soll das unbefugte Integrieren von Nodes verhindern. Jeder Knoten verfügt über einen automatisch oder manuell vergebenen Namen. Über diesen kann man Prozesse auf entfernten Nodes starten oder vorhandene ansprechen. Bis auf diesen Namen unterscheiden sich der lokale und der entfernte Nachrichtenversand nicht. Das Marshalling der Daten erfolgt für den Nutzer vollkommen transparent. Zusätzlich zu den Spracheigenschaften unterstützen mitgelieferte Module die Arbeit mit Prozessen auf unterschiedlichen Knoten. Auf diese Weise sind verteilte Systeme leicht zu implementieren.

Diverse weitere Eigenschaften erleichtern die Entwicklung von Anwendungssystemen. Supervisor Trees können Prozesse automatisch informieren, wenn ein Kindprozess stirbt, Gleiches lässt sich manuell über Links oder Monitors erreichen, ebenfalls wieder über Node-Grenzen hinweg oder für ganze Nodes. So kann eine Anwendung Fehler korrigieren oder automatisch die Funktionen eines fehlerhaften Knotens übernehmen. Konstrukte für die Ausnahmebehandlung sowie die Fähigkeit, Software-Upgrades zur Laufzeit durchzuführen, erhöhen die Stabilität und Systemlaufzeit zusätzlich.

Mehr als nur eine Programmiersprache

Eine Programmiersprache mit ihren Eigenschaften ist nur eine Hälfte dessen, was den Einsatzzweck und den Erfolg einer Plattform ausmacht. Heutzutage beurteilt man eine

Listing 7

```
-module(module_g).
-export([server_test/0]).
server_test() ->
    module_f:start(0),
    my_server ! {do_this, 4711, foo},
    my_server ! {do_that, bar},
    my_server ! stop.
```

Nachrichten lassen sich an die Prozess-ID oder einen registrierten Namen senden.

Sprache immer im Zusammenhang mit ihren Bibliotheken und Laufzeitumgebungen. Dies gilt auch für Erlang. Neben einer Vielzahl hilfreicher Module bietet das System unter dem Namen Open Telecom Platform (OTP) und den dazugehörigen OTP Design Principles spezielle Module und Vorgaben für die komfortable Entwicklung skalierbarer und robuster Anwendungssysteme.

Wesentliche Bestandteile der Design Principles sind Supervisor Trees und Behaviours. Supervisor Trees informieren sich gegenseitig, sollte in einer Umgebung mit verknüpften Prozessen einer der Prozesse ausfallen. Erlang unterscheidet zwei Prozesstypen: Die einen arbeiten (Worker), und die anderen passen auf sie auf (Supervisor). Oftmals kommen in einem Supervisor Tree viele Prozesse mit gleichartigen Strukturen zum Einsatz, zum Beispiel als Server oder als Event Handler. Diese Ähnlichkeiten werden über Behaviours formalisiert.

Beim Aufruf einer Funktion aus einem anderen Modul kann auch eine Variable den Namen des aufrufenden Moduls festlegen. Dies machen sich viele Erlang-Module zu Nutze, um Grundfunktionen ähnlich zu abstrakten Oberklassen in der objektorientierten Programmierung in generische Module auszulagern. Ein eigenes Modul, das ein solch generisches Modul nutzen soll, muss nur vorgegebene Funktionen implementieren und seinen eigenen Namen als Argument an die Funktionsaufrufe des generischen Moduls übergeben. Dieses verwendet für seine Arbeit nun die Funktionen des eigenen Moduls. Der Mechanismus hierfür heißt Callback. Über Behaviours kann ein generisches Modul festlegen, welche Funktionen ein Callback-Modul zu implementieren hat. Fehlen diese, gibt der Compiler eine Warnung aus.

Eine Erlang-Applikation wird über das gleichnamige Modul und seine Konfiguration festgelegt. Ein Callback-Modul definiert die Funktionen für den Start und den Stop der Anwendung, oftmals nur für den Start eines Supervisors. Gleichzeitig definiert eine Konfiguration in der Erlang-typischen Notation aus Tupeln und Listen dieses Callback-Modul. Die Konfigurationsdatei enthält die Beschreibung des Moduls, seine Version, darin registrierte Prozesse sowie in ihm enthaltene weitere Anwendungen und Konfigurationen. Der Start der Applikation erfolgt in der mitgelieferten Shell per *application:start(app_name)*. Über das System-Init lässt sich dieser Vorgang automatisieren.

Für die Erstellung ganzer Distributionen mit einer Teilmenge des Systemumfangs kommen Releases zum Einsatz. Nach der Definition des Release Resource File erzeugt *systools* das Boot Script sowie die Release Packages. Die resultierende TAR-Datei enthält alle notwendigen Dateien für das System mit den parallel laufenden Applikationen.

Die Callbacks des Supervisor-Moduls zum Aufbau des Prozessbaums definieren nur die Funktion *init(Args)*, die die Konfiguration der verwalteten Supervisor und Worker festlegt. Sie definiert, ob die Prozesse einmalig oder permanent laufen, ob sie einzeln oder alle im Fehlerfall neu gestartet werden, wie sie gestoppt werden und in welcher Frequenz ein Prozess terminieren darf, bevor der Supervisor selbst seine Arbeit been-

det. Allein dies sorgt bereits für stabile Systeme.

Hingegen werden die Worker als Callbacks für das Modul *gen_server* ausgelegt. Sie müssen Funktionen für die Initialisierung und Terminierung, für die Verarbeitung synchroner und asynchroner Nachrichten sowie für den Umgang mit Updates im laufenden Betrieb implementieren. Ein Mechanismus zur Verwaltung von Zuständen ist enthalten. Insgesamt entbindet dieses Modul den Entwickler von stupider Low-Level-Arbeit bei der Entwicklung eigener Server-Prozesse.

Weitere interessante Module der OTP bieten eine generische Event Engine inklusive vorgefertigter Handler-Module für Logging und Warnmeldungen sowie einen generischen endlichen Automat. Ferner gibt es Mechanismen für die Verteilung von Applikationen auf unterschiedliche Nodes inklusive eines prioritätsgesteuerten automatischen Takeover und Failover von Prozessen. Schließlich erfolgen über Konfigurationsdateien gesteuerte automatische Updates von Applikationen und Releases. Alles zusammen beschert dem Ericsson AXD301 ATM Switch eine nahezu unglaubliche Verfügbarkeit von 99,9999999 Prozent (9NINES).

Module für fast alle Aufgaben

Außerhalb der OTP gehören noch viele weitere hilfreiche Module zum Lieferumfang von Erlang. Heutzutage unumgänglich ist eine umfangreiche Netzbibliothek. So deckt Erlang von TCP und UDP über SSL und SSH bis HTTP, FTP und TFTP alle wichtigen Protokolle ab, zudem unterstützt die Plattform das Media Gateway Control Protocol (Megaco)/H.248. Weiterhin befinden sich viele Module rund um CORBA und SNMP im Lieferumfang. Zusammen mit den vorhanden Kryptofähigkeiten (unter anderem MD5, SHA, DES, AES, RSA, DSS) lassen sich so leistungsfähige Server- und Clientlösungen implementieren.

Für die in diesen Systemen oftmals benötigten persistenten Daten stehen ebenfalls unterschiedliche Lösungen zur Verfügung. Sind nur einfache Daten zu speichern, kann man ein eigenes Modul für einfache Tabellen im Dateisystem implementieren, sollen hierfür hingegen relationale Datenbanksysteme zum Einsatz kommen, erfolgt der Zugriff über ODBC. Wer kein Drittsystem integrieren muss, kann auf Erlangs mitgeliefertes DBMS Mnesia zurückgreifen. Das leistungsfähige System ist auf den kontinuierlichen Betrieb mit nahezu Echtzeitverhalten ausgelegt, verfügt über ein hybrides Datenmodell für Relationen und Objekte, kennt unterschiedliche Strategien, lässt sich replizieren und fragmentieren und bettet sich mit seiner API für Transaktionen und Abfragen nahtlos in Erlang ein.

Weitere Module unterstützen den Entwickler mit unterschiedlichen Speicherstrukturen, der Verarbeitung regulärer Ausdrücke, ASN.1 und LALR-1, dem Lesen und Schreiben von ZIP-Dateien, dem Zugriff auf die Windows-Registry, Prozess-Spooling, Heartbeats und einem einfachen Grafiksystem. Auch für die eigentliche Entwicklungsarbeit bringt Erlang eine Vielzahl von Werkzeugen mit. Eine eigene IDE fehlt zwar, jedoch gibt es eine direkte Unterstützung für den Emacs. Neben dem Compiler und einer Shell für die interaktive Ausführung bringt Erlang integrierte Applikationen für das Debugging, Unit Testing, Cross References, Coverage, Profiling, die Generierung von Dokumentationen, Process Monitoring, Application Monitoring, Crashdump Analysis und Scripting mit. Einige dieser Applikationen führt das System zeichenorientiert in der Shell aus, andere verfügen über ein grafisches Frontend oder lassen sich im Webbrowser betrachten.

Wem dies nicht genügt, dem stehen eine Vielzahl weiterer Bibliotheken und Applikationen im Netz zur Verfügung. Aus dem Comprehensive Erlang Archive Network (CEAN) beispielsweise lassen sich Anwendungen direkt in die Laufzeitumgebung installieren oder aktualisieren.

Erlang/OTP ist eine Nischenplattform, aber aus der Nische entwickelt sich entsprechend dem Bedarf an skalierbarer Software in Multicore-/Multiprozessor-Umgebungen langsam eine immer interessanter und bekannter werdende Menge an Lösungen. Natürlich findet sich Erlang in seinem ursprünglichen Anwendungsgebiet wieder, dem Ericsson AXD301 ATM Switch, dem Ericsson GPRS System, dem Alteon (Nortel) SSL Accelerator, dem T-Mobile UK SMS System, und auch Motorola hat die Plattform für VoIP-Lösungen evaluiert. Mit Yaws existiert ein hoch skalierbarer und flexibler Web Application Server für statische und dynamisch generierte Seiten. Der Server wird in verschiedenen Softwaresystemen produktiv eingesetzt. Ein im Jabber-Umfeld gern genutzter Daemon ist der *ejabberd*, der ebenfalls in Erlang entwickelt wurde. Interessante Datenbanklösungen sind die CouchDB, die eine RESTful-HTTP/JSON-API bietet und so von jeder Sprache aus leicht zu nutzen ist, sowie Amazons SimpleDB. Im Grafiksektor findet sich mit Wings 3D eine auf Erlang basierende Applikation. Last but not least steht für Entwickler mit Tsung ein Multi-Protocol Distributed Load Testing Tool zur Verfügung.

Onlinequellen

Erlang	www.erlang.org
Ericsson	www.erlang.se
CEAN	cean.process-one.net

Fazit

Die zukünftige Verbreitung von Erlang ist schwer einzuschätzen. Der Bedarf an auf Parallelverarbeitung basierenden Anwendungssystemen steigt, die Anzahl der hierfür zur Verfügung stehenden Plattformen ist überschaubar. Erlang ist nach inzwischen 20 Jahren Entwicklungszeit mit dem Release R12B stabil und ausgereift und erlaubt kompakte, robuste und skalierbare Lösungen. So betrug der Erlang-Codeumfang der Evaluierung bei Motorola weniger als 25 Prozent des C++-Codes. Allerdings erscheint die Notation vielen Entwickler gewöhnungsbedürftig, was sicherlich eine Hürde darstellt.

Dafür wird Erlang jedoch seinen Einfluss auf Alternativen haben. Inwiefern diese auf Java oder .Net basieren, oder es sich um komplett eigenständige Entwicklungen handelt, bleibt abzuwarten. Viele der positiven Eigenschaften sind nicht in der Sprache, sondern der VM begründet. Leichtgewichtige Prozesse, asynchrones Messaging, nicht modifizierbare Variablen – dies muss eine Alternative schon bieten. Vielleicht wäre hier eine Sprache im C-Style mit einer direkten Übersetzung nach Erlang der erfolgreichere Ansatz. (ka)

FRANK MÜLLER

arbeitet als Teamleiter und Senior Consultant bei der BTC Business Technology Consulting AG in Oldenburg.

Literatur

[1] Joe Armstrong; Programming Erlang; Software for a Concurrent World; Pragmatic Programmers, Juli 2007







SPML: Standard für Identity Provisioning

Multiple Profile

Martin Raepple

In komplexen IT-Umgebungen besitzen Anwender viele Persönlichkeiten. Wer die zahlreichen Identitäten über System- und Unternehmensgrenzen hinweg in den Griff bekommen will, braucht leistungsfähige Konzepte. Als offener Standard soll die Service Provisioning Markup Language die entsprechenden Prozesse automatisieren.

Netzwerkzugang, E-Mail-Adresse oder Zutrittskarte: alles grundlegende Voraussetzungen, ohne die der reibungslose Ablauf vieler Unternehmensprozesse nicht möglich wäre. Das tritt häufig erst dann ins Bewusstsein, wenn man die genannten Dinge beispielsweise nach einem Job- oder Projektwechsel neu beschaffen muss. Dann heißt es Anträge ausfüllen oder erst einmal die Zugangsdaten des Kollegen mitbenutzen, bis die IT-Abteilung das Benutzerkonto eingerichtet hat. In diesen Versorgungsprozessen, allgemein unter dem Begriff Provisioning zusammengefasst, steckt meist viel Handarbeit und ein entsprechend hoher administrativer Aufwand. Inkonsistente Datenbestände, lange Wartezeiten und eine frustrierte Anwenderschaft sind oft die Folge.

Die stetig wachsende Anzahl von Benutzerkonten pro Mitarbeiter sowie regulatorische Vorgaben zur Erhöhung des Sicherheitsniveaus zählen zu den wichtigsten Gründen, warum sich das systemgestützte Verwalten digitaler Identitäten (Identity Management) in den vergangenen Jahren zu einem der bedeutendsten Anwendungsgebiete für das Provisioning entwickelt hat. Das User oder Identity Provisioning zählt neben einer unternehmensweiten Rollenverwaltung und Steuerung von Freigabeprozessen für den Zugriff auf Ressourcen zu den zentralen Funktionen moderner Identity-Management-Systeme. Über Letztere erhalten Angestellte von zentraler Stelle aus Zugang zu den Anwendungssystemen entsprechend ihrer Rolle in der Organisation.

Konkret befasst sich das Identity Provisioning mit dem Automatisieren aller Vorgänge, die den Lebenszyklus digitaler Identitäten steuern (Erstellen, Ändern, Deaktivieren, Löschen). Ein typischer Anwendungsfall ist die Einstellung eines neuen Mitarbeiters, dessen Stammdaten zunächst im Personalsystem erfasst werden. Er benötigt in der Regel Benutzerkonten in mehreren Systemen, was in historisch gewachsenen IT-Landschaften regelmäßig komplizierte technische Verteilungsprozesse auslöst.

Sicher durch saubere Konten

Identity Provisioning kann dafür sorgen, dass diese Vorgänge schnell, konsistent und nachvollziehbar bleiben. Gleiches gilt bei sich ändernden Aufgaben und Positionen sowie dem Entzug aller Berechtigungen (De-Provisioning), wenn ein Mitarbeiter die Firma verlässt. Laut einer aktuellen Sicherheitsstudie, die dem Identitätsdiebstahl mittels Phishing, Password Stealern, Keyloggern und anderen Angriffswerkzeugen ein hohes Risiko bescheinigt, liefern durchgängig automatisierte Versorgungsprozesse auch einen wesentlichen Beitrag zur

iX-TRACT

- Identity Provisioning kümmert sich um alle Prozesse, die für die Administration verteilter Benutzerinformationen notwendig sind.
- Als offener Standard definiert die Service Provisioning Markup Language (SPML) ein herstellerübergreifendes XML-Protokoll zur Steuerung des Lebenszyklus beliebiger IT-naher Ressourcen.
- SPML wird hauptsächlich im Identity Provisioning eingesetzt. Hier gibt es etliche kommerzielle Implementierungen des Standards sowie eine aktive Open Source Community.

Verbesserung der Informationssicherheit im Unternehmen: Ungenutzte Benutzerkonten lassen sich sofort deaktivieren und dienen so nicht länger als Einfallstore für interne oder externe Angriffe (siehe *iX*-Link am Ende des Textes oder den Kasten „Onlinequellen“). Weitere Anwendungsfelder für das Identity Provisioning finden sich im User-Help-Desk. Dazu gehört beispielsweise das Zurücksetzen von Passwörtern, das der Anwender selbst initiieren und weitgehend automatisiert durchführen darf.

Die Kommunikation zwischen den zahlreichen Provisionierungslösungen und den Zielsystemen, deren Benutzerkonten und Berechtigungen zentral verwaltet werden sollen, erzeugt einen hohen Integrationsaufwand. Dem Artenreichtum an Datenbanken, Verzeichnisdiensten und anwendungsspezifischen Benutzerverwaltungen in einer heterogenen Umgebung versuchen die Hersteller mit plattformspezifischen Konnektoren oder lokalen Agenten zu begegnen, und können dennoch in der Regel keine vollständige Abdeckung aller Zielsysteme erreichen. Ordnung in das babylonische Sprachgewirr aus Protokollen und Formaten will das Standardisierungsgremium OASIS mit der Service Provisioning Markup Language (SPML) bringen. Die in der zuständigen Arbeitsgruppe (Provisioning Services Technical Committee, PSTC) vertretenen Firmen wie BMC, CA, SAP und Sun hatten bereits 2003 die erste Version zu Papier gebracht. Drei Jahre später folgte die umfangreich überarbeitete Spezifikation zu SPML 2.0.

Hauptanliegen der Sprache ist es, die Funktionen für die Provisionierung, deren Syntax und Nachrichtenprotokoll plattformübergreifend zu vereinheitlichen. SPML bedient sich dazu bei den üblichen Verdächtigen: Die auf einem einfachen Request/Response-Protokoll basierenden Operationen werden mit XML formuliert und in SOAP-Nachrichten für den Transport eingebunden. Version 1.0 spezifizierte lediglich eine Menge an Basisoperationen. 2.0 fasst diese zu den Core Operations zusammen und erweitert sie um sogenannte Capabilities, die weitere optionale, fachlich verwandte Funktionen eines Provisionierungssystems beschreiben (siehe Tabelle „Provisionierungsoperationen in SPML 2.0“). Wem das nicht genügt, der kann sich bei den Extended Operations in SPML 1.0 beziehungsweise den Custom Capabilites in SPML 2.0 bedienen, die ein formales Modell des Standards für produktspezifische Erweiterungen definieren.

Provisionierungsoperationen in SPML 2.0

Eigenschaft	Beschreibung	Operationen
Core Operations	Basisoperationen, die jede standardkonforme Implementierung unterstützen muss	*add, lookup, modify, delete, listTargets*
Async Capability	asynchrone Verarbeitung von SPML Requests	*cancel, status*
Batch Capability	Stapelverarbeitung von mehreren SPML Requests	*Batch*
Bulk Capability	Bearbeitung mehrerer PSOs in einem SPML Request	*bulkModify, bulkDelete*
Password Capability	Operationen zum Prüfen und Ändern von Passwörtern	*setPassword, expirePassword, resetPassword, validatePassword*
Search Capability	Suchoperation, die einen Iterator zur schrittweisen Abarbeitung des Suchergebnisses liefert	*search, iterate, closeIterator*
Suspend Capability	Aktivieren und Deaktivieren von PSOs	*suspend, resume, active*
Updates Capability	gleiche Funktion wie die Bulk-Operationen, liefert aber einen Iterator zur schrittweisen Abarbeitung der von der Änderung betroffenen PSOs zurück	*updates, iterate, closeIterator*
Reference Capability	ermöglicht die Definition von Beziehungen zwischen PSOs (zum Beispiel Gruppenmitgliedschaften von Benutzern) auf generische Weise, das heißt unabhängig von deren Schema. Reference Capability definiert keine eigenen Operationen, sondern lässt sich mit den Basisoperationen anwenden.	

Ein Protokoll für alle

Über die Inhalte der mit den Nachrichten übertragenen Objekte, im SPML-Jargon als Provisioning Service Objects (PSOs) bezeichnet, trifft die Spezifikation keine Aussagen. Dagegen spricht zum einen der Wunsch nach einem universellen Protokoll, das nicht nur den Lebenszyklus von Benutzerkonten und Berechtigungen steuern soll. Zum anderen ist es selbst für ein abgrenzbares Anwendungsgebiet wie das Identity Provisioning nur schwer möglich, ein industrie- und branchenweit gültiges Datenmodell für Benutzer und deren Attribute verbindlich festzulegen. Die Unterschiede auf semantischer und struktureller Ebene sind hier so groß, dass ein Standard allenfalls eine Empfehlung aussprechen kann, an der das PSTC gerade arbeitet (SPML Standard Schema).

Dennoch sieht die Spezifikation vor, dass jedes Zielsystem von Provisionierungsanfragen, formal als Provisioning Service Target (PST) bezeichnet, die Datenmodelle der von ihm verwalteten PSOs beziehungsweise Identitäten über XML Schema (XSD) beschreiben kann. Andere Teilnehmer können die vom PST unterstützten Identitätsschema über die Core Operation *listTargets* in Erfahrung bringen, um anschließend entsprechende SPML Requests (zum Beispiel Anlegen eines neuen Benutzerkontos) mit den richtigen Attributen zu formulieren. Für einfache Datenstrukturen steht als Alternative zu XSD eine eigene, schon mit Version SPML 1.0 eingeführte Schemasprache zur Verfügung, deren Wortschatz sich aber im Wesentlichen auf die einfache Deklaration von Attributen beschränkt.

Neben PSOs und PSTs zählen zwei weitere Komponenten zu dem auf abstrakter Ebene beschriebenen Domänenmodell, das die grundsätzliche Rollenverteilung und Beziehung zwischen den Teilnehmern in einem durchgängigen Provisionierungsszenario regelt (Abbildung 1). In der Rolle der sogenannten Requesting Authority initiiert ein Personalsystem im gewählten Beispiel den Versorgungsprozess und schickt standardkonforme Provisionierungsanfragen (SPML Requests) an einen Provisioning Service Provider (PSP), den üblicherweise ein zentrales Identity-Management-System bereitstellt. Der PSP nimmt die Anfrage entgegen und führt sie aus unter Einbindung der von ihm verwalteten PSTs (Verzeichnisdienste, Datenbanken et cetera).

Autorität in den Prozessen

Abhängig vom gewählten Verarbeitungsmodus lässt der PSP die Requesting Authority solange auf die Rückmeldung (*SPML Response*) warten, bis alle von der Anfrage betroffenen PSTs ihrerseits die Arbeit beendet haben (synchrone Verarbeitung). Mit SPML kann die Requesting Authority durch Angabe des optionalen Attributs *executionMode='asynchronous'* eine asynchrone Variante der Operation beim PSP anfordern, was diesen dazu veranlasst, zunächst nur mit einer kurzen Empfangsbestätigung zu antworten und erst im Anschluss mit der Bearbei-

Listing 1

```
<spml:addRequest targetID="Portal"
  xmlns:spml="urn:oasis:names:tc:SPML:2:0">
  <spml:data>
    <user>
      <name>John Smith</name>
      <id>jsmith</id>
      <email>john.smith@acme.com</email>
      <phone>
        <home>12345</home>
        <work>54321</work>
      </phone>
    </user>
  </spml:data>
</spml:addRequest>
@bu:Anlage eines Benutzerkontos mit SPML Add Request
(Listing**1)
```

Anlage eines Benutzerkontos mit SPML Add Request

Listing 2

```
<spml:addResponse status="spml:success"
  xmlns:spml="urn:oasis:names:tc:SPML:2:0" />
  <spml:pso>
    <spml:psoID ID="4711" targetID="portal"/>
  </spml:pso>
</spml:addResponse>
@bu:SPML Add Response des Provisioning Service Provider
(Listing**2)
```

SPML Add Response des Provisioning Service Provider

tung zu beginnen. Über die *status*-Operation ist die Requesting Authority jederzeit in der Lage, den aktuellen Bearbeitungsstand abzufragen und mit *cancel* die Ausführung vorzeitig zu stoppen.

Listing 1 zeigt einen exemplarischen SPML Request, der ein neues Benutzerkonto (PSO) über die Core Operation *add* auf dem Zielsystem (PST) mit der eindeutigen Bezeichnung (*targetID*) „Portal“ anlegt. Die zugehörigen Identitätsdaten werden als XML-Dokument mit dem Wurzelelement *<user>* übergeben und müssen dem gültigen Datenmodell des PSOs entsprechen. Das zugehörige XML Schema besorgt sich die Requesting Authority zuvor über die Basisoperation *listTargets*.

Da alle Interaktionen zwischen den logischen Komponenten im SPML-Domänenmodell auf einem Request/Response-Protokoll beruhen, quittiert der PSP den *addRequest* mit der zugehörigen *addResponse* (Listing 2). Die gibt Auskunft über den aktuellen Bearbeitungsstatus (*success*, *failure* oder *pending*) und liefert bei synchroner Ausführung zudem das vom PST vergebene Kennzeichen (*psoID*) mit, unter dem sich das PSO nach dem erfolgreichen Erstellen in allen nachfolgenden Provisionierungsoperationen (etwa der Zuordnung von Berechtigungen) eindeutig referenzieren lässt.

SOAP über HTTP ist die geläufigste Variante für den Austausch von SPML-Nachrichten. Alle erhältlichen Implementierungen unterstützen dieses in SPML als SOAP/HTTP Binding bezeichnete Transportverfahren, das den SPML Request beziehungsweise die SPML Response im SOAP Body übermittelt. Das schafft Vorteile: Zum einen lassen sich die Nachrichten mit allen etablierten Sicherungsmechanismen für Webservices auf Transport- und Nachrichtenebene schützen [1], zum anderen ermöglichen standardisierte Nachrichten und Transportprotokolle die unternehmensübergreifende Versorgung mit Identitätsdaten (Federated Identity Provisioning). Angesichts immer stärker verzahnter Lieferketten lassen sich so beispielsweise Systeme bei Lieferanten und Partnern in die Provisionierungsprozesse einbinden. Mit proprietären Konnektoren ist das kaum zu bewerkstelligen.

Die Rollen nach dem SPML-Domänenmodell sollen den Aufbau eines systemunabhängigen Provisionierungsszenarios erlauben (Abb. 1).

Unterstützung ist gefragt

Im Idealfall unterstützen alle logischen Komponenten des SPML-Domänenmodells das Protokoll. Derzeit fühlt sich jedoch vorrangig die überschaubare Gemeinde der Hersteller von Identity-Management-Systemen wie Sun (Java System Identity Manager), CA (eTrust Admin) oder Beta Systems (SAM Virtual Directory) berufen, standardkonforme SPML-Schnittstellen in ihren Produkten anzubieten. Nicht ohne Grund, denn schließlich verspricht der breite Einsatz von SPML, den Aufwand für das Entwickeln plattformspezifischer Konnektoren und Agenten zu reduzieren. Die Anwendungsanbieter halten sich dagegen noch bedeckt. SAP bietet als einer der wenigen die Möglichkeit, die Benutzer- und Rollenverwaltung im Netweaver Application Server Java ab Version 6.40 über eine SPML-1.0-Schnittstelle zu steuern. Streng genommen nimmt ein solches Zielsystem (PST), das SPML direkt verarbeiten kann, in einer Doppelrolle auch die Funktionen eines PSP wahr. Gleiches gilt für ein Identity-Management-System beziehungsweise PSP, das zugleich als Requesting Authority agiert, wenn es nicht nur eingangsseitig SPML akzeptiert, sondern auch ausgangsseitig über das Protokoll mit den PSTs kommuniziert.

Um SPML-fähige Clients ist es zumindest unter Java gut bestellt. Das quelloffene OpenSPML Toolkit lässt sich unter den Bedingungen der Common Development and Distribution License (CDDL) in Java-Anwendungen als Requesting Authority einbinden. Sein für beide Versionen des Standards verfügbares Java-Archiv (JAR) liefert die notwendigen Klassen, die auf Objektebene SPML Requests erzeugen beziehungsweise die Antworten des PSP als Objekte erhalten, ohne dass man sich um die aufwendige Serialisierung/Deserialisierung kümmern muss. Neben jeweils eigenen Klassen für die Anfrage und Antwort zu jeder Operation (zum Beispiel *AddRequest*, *AddResponse*) steht ein fertiger SOAP Client zur Verfügung, der die Nachrichten, wie im SOAP/HTTP Binding beschrieben, an einen PSP schicken kann. Listing 3 zeigt, wie sich mit dem OpenSPML Toolkit der Benutzer mit der eindeutigen ID *jsmith* der Gruppe *Administrators* mittels *modify*-Operation zuordnen lässt. Es handelt sich um eine Provisionierungsanfrage an ein SAP-System [2].

Nur an einer Stelle weist der Code ein plattformspezifisches Merkmal auf: Das Attribut, über dessen Inhalt sich die Benutzerzuordnung verwalten lässt, trägt die Bezeichnung *member*. Diese auf der Grundlage von PST-eigenen Identitätsattributen vorgenommene Assoziation zwischen zwei Provisioning Service Objects (hier Benutzer und Gruppe) hat man als grundsätzliches Problem von SPML 1.0 erkannt und in der aktuellen Version durch die generische Reference Capability behoben. Nach Zuordnung des Benutzers *jsmith* zum richtigen Gruppenattribut im Konstruktor der Klasse *Modification* erhält der PSP über die Methode *setOperation* die Nachricht, dass es sich um eine Erweiterung der Gruppenmitgliedschaften handelt (OP_ADD). Ohne weiteres Zutun kann das *modifyRequest*-Objekt nun mit seiner Methode *toXML()* dafür sorgen, dass eine standardkonforme SPML-

Listing 3

```
ModifyRequest modifyRequest = new ModifyRequest();
Identifier identifier = new Identifier();
identifier.setType(Identifier.TYPE_GenericString);
identifier.setId("GRUP.PRIVATE_DATASOURCE.un:Administrators");
modifyRequest.setIdentifier(identifier);
Modification modification = new Modification("member",
  "USER.PRIVATE_DATASOURCE.un:jsmith");
modification.setOperation(Modification.OP_ADD);
modifyRequest.addModification(modification);
```

@bu:Zuordnung eines Benutzers zu einer Gruppe mit dem OpenSPML Toolkit (Listing**3)

Zuordnung eines Benutzers zu einer Gruppe mit dem OpenSPML Toolkit

Listing 4

```
<spml:modifyRequest xmlns:dsml="..." xmlns:spml="...">
  <spml:identifier xmlns:spml=""
    type="urn:oasis:names:tc:SPML:1:0#GenericString">
    <spml:id xmlns:spml="">
      GRUP.PRIVATE_DATASOURCE.un:Administrators
    </spml:id>
  </spml:identifier>
  <spml:modifications xmlns:spml="">
    <dsml:modification name="member" operation="add">
      <dsml:value xmlns:dsml="">
        USER.PRIVATE_DATASOURCE.un:jsmith
      </dsml:value>
    </dsml:modification>
  </spml:modifications>
</spml:modifyRequest>
```

@bu:Serialisierter SPML 1.0 Request (Listing**4)

Serialisierter SPML 1.0 Request

Nachricht erzeugt wird (Listing 4).

Fazit

SPML erleichtert die Verwaltung verteilter Benutzerinformationen in komplexen Systemen. Die Sprache adaptiert verwandte Sicherheitsstandards wie SAML (Security Assertion Markup Language) [3] und XACML (eXtensible Access Control Markup Language) für die plattformübergreifende Formulierung von Berechtigungsregeln und schließt eine wichtige Lücke beim Identity Provisioning. Trotz ihrer Akzeptanz bei den Herstellern von den Identity-Management-Systemen wäre es gut, wenn sich die Anbieter von Applikationsservern hier anschließen würden. Denn ihre Produkte spielen eine zentrale Rolle für das Identity Provisioning. Zurzeit arbeitet OASIS an einem Enterprise Provisioning Profile, das analog zu den Richtlinien der Web-Services-Interoperability-Organisation eine bessere Zusammenarbeit zwischen den unterschiedlichen Implementierungen des Standards definieren soll. (jd)

MARTIN RAEPPLE

ist Koautor von SPML 2.0 und vertritt die SAP AG bei OASIS und anderen Gremien im Bereich Webservices und Security.

Literatur

[1] Martin Raepple; Web Services; Dreiklang; WS-Security: Neue Standards für mehr Sicherheit; *iX* 5/2006, S. 126
[2] Martin Raepple; Programmierhandbuch SAP NetWeaver Sicherheit; SAP Press, 2008
[3] Christian Mezler-Andelberg; Webidentität; Ich und Ich; Weichenstellung für das Identity-Management; *iX* 10/2007, S. 124


iX-Link ix0806120

Onlinequellen

Studie zur Sicherheit im Internet
www.ibm.com/services/us/iss/pdf/etr_xforce-2007-annual-report.pdf

OASIS Provisioning Services Technical Committee
www.oasis-open.org/committees/tc_home.php?wg_abbrev=provision

Service Provisioning Markup Language (SPML 1.0)
www.oasis-open.org/specs/index.php#spmlv1.0

Service Provisioning Markup Language (SPML 2.0)
www.oasis-open.org/specs/index.php#spmlv2.0

OpenSPML Toolkit
www.openspml.org



Rails-Tutorial I: Einrichten und anpassen

Außergewöhnlich auf Schienen

Denny Carl

Die professionelle Entwicklung von Webanwendungen erleichtern Web-Frameworks wie das immer beliebtere Ruby on Rails. Das MVC nutzende Framework propagiert unter anderem Konventionen einzuhalten statt zu konfigurieren.

Ruby on Rails hat mächtig Fahrt aufgenommen, wenngleich die Begeisterung in hiesigen Entwicklerkreisen im Vergleich zu den USA oder Großbritannien eher zurückhaltend ist. Das mit diesem Artikel beginnende Tutorial beschäftigt sich mit der Entwicklung einer realen Webapplikation und soll zeigen, dass sich der Einstieg und Umstieg auf Ruby on Rails und damit auf effizientes, gut organisiertes Coding für das Web aus einem Guss lohnt.

Mit dem Tutorial entsteht *Trainspotr*, eine Community für Menschen, die in ihrer Freizeit auf der Jagd nach teils seltenen, teils alltäglichen Zügen und Lokomotiven gehen und dies mit Fotos dokumentieren. Das erlaubt einen Einblick in die Entwicklung einer datenbankgestützten Anwendung mit Rails und die Implementierung von Features wie durch Login geschützte Bereiche, Datei-Upload, Bewertungen und Geotagging. Zudem zeigt sich bald, wie gekonnt Ajax in Ruby on

Rails eingeflochten ist und wie schnell ein Admin-Bereich zur internen Pflege der Nutzerdaten dank Scaffolding entsteht. In diesem ersten Teil geht es um das Einrichten einer Rails-Anwendung, das Verwalten von Daten in einer Datenbank und deren Darstellung im Browser.

„Trainspotter“ und Rails-Entwickler haben eines gemeinsam: Die Begeisterung für die Schiene. Für Züge sind Schienen der fest vorgegebene Weg ihrer Reise, auf denen sie eine hohe Geschwindigkeit erreichen können, wenn sie geradlinig verlaufen und die Züge nicht so oft abbremsen müssen. So ist das auch bei Rails: Es ist ein Framework für Webapplikationen, das dem Entwickler durch ein ausgeklügeltes Konzept und einige Konventionen den Weg weist. Ein Rails-Entwickler braucht ebenfalls selten zu bremsen, denn Rails bringt viele Features, die moderne Webapplikationen benötigen, gleich mit. Sogar Javascript oder SQL kann man mit Ruby und damit ohne Bremsverluste einbinden.

Was an Rails so besonders ist

Rails verfolgt das MVC-Pattern (Model – View – Controller), wodurch der gesamte Programmcode sauber strukturiert und leicht zu pflegen ist. Während sich die Geschäftslogik der Anwendung in einem Model niederschlägt, erhält die View-Ebene den nötigen Quelltext zur Anzeige von Daten. Ein Controller koordiniert die Zusammenarbeit, holt Daten und weist sie zur Anzeige an.

Neben MVC ist DRY ein weiteres Zauberwort bei Rails-Entwicklern. Es steht für „Don’t Repeat Yourself“ und umfasst Funktionen und Konzepte, die es erleichtern, sich wiederholende Quelltextteile zu vermeiden.

Durch den Grundsatz „Convention over Configuration“ sparen sich Rails-Entwickler das oftmals lästige und zeitaufwendige Hinterlegen von Daten, die das Zusammenwirken von einzelnen Programmteilen beschreiben. Rails setzt ein paar einfach zu verinnerlichende Regeln voraus, an die sich der Entwickler halten sollte, möchte er ohne Umwege schnell ans Ziel kommen. So erwartet es beispielsweise einen Zusammenhang zwischen der Bezeichnung eines Model und einer Datenbanktabelle, mit der es in Verbindung steht. Diesen Zusammenhang muss somit niemand festhalten. Zu nutzende Bibliotheken oder einzelne Ruby-Dateien werden automatisch und ohne eine Zeile Code geladen – sofern sie sich an der richtigen Position befinden.

Eine Rails-Anwendung kann standardmäßig in drei Umgebungen laufen: *development*, *test* und *production*. Dies wirkt sich beispielsweise auf den Umfang von Fehlermeldungen – wichtig während der Entwicklung – oder die Intensität des Cachings von Daten aus, was erst im produktiven Einsatz wichtig ist. Die Test-Umgebung setzt den gesamten Datenbestand bei jedem Testlauf zurück, um stets eine gleiche Ausgangsbasis für die durchzuführenden Tests zu gewährleisten. Jede Umgebung erhält ihre eigene Datenbank und schreibt zudem eigene Log-Dateien.

Weitere produktive Bestandteile im Rails-Framework sind die diversen, standardmäßig eingebauten Tests, Code-Generatoren und Meta-Programmierelemente. Außerdem erweitern Plug-ins die Fähigkeiten von Rails gezielt. Rails-Anwendungen können nicht nur HTML, sondern eine ganze Reihe von Formaten zur Ausgabe nutzen, was die Bereitstellung von Webservices stark erleichtert.

Einfaches Einrichten der Umgebung

Ein praktisches Nachvollziehen des Tutorials setzt eine Umgebung voraus, die über die aktuellen Ruby- und Rails-Versionen (1.9 beziehungsweise 2.0), sowie den Paketmanager RubyGems und das an das C-Entwicklern bekannte *make* angelehnte Rake verfügt. Wie man seinen Rechner „auf die Schienen“ setzen kann, erläutern viele betriebssystemspezifische Anleitungen im Netz (siehe „Onlinequellen“).

Für Windows-Entwickler lohnt der Blick auf die schnell einsatzfähige Komplettlösung InstantRails, durch die Ruby, Rails, Apache, MySQL sowie Tools und Codebeispiele mit wenigen Klicks und in aktuellen Versionen einsatzbereit sind. Mac OS X 10.5 bringt Rails von Haus aus mit.

Es ist angebracht, vor dem Start der Entwicklung einer Rails-Anwendung alle beteiligten Komponenten auf Updates zu überprüfen. RubyGems überträgt die neueste stabile Rails-Version durch *gem update rails* auf den eigenen Rechner – per Kommandozeile.

Gerüst mit Verzeichnissen

Jede Rails-Anwendung besteht zunächst aus einem Grundgerüst aus Verzeichnissen und Dateien. Dies generiert der Befehl *rails*, dem der Name der Anwendung übergeben wird. Anschließend erzeugt das Framework ein Unterverzeichnis mit diesem Namen. Des Weiteren erstellt es die Verzeichnisstruktur der Anwendung, kopiert benötigte Dateien und setzt die Konfigurationseinstellungen auf Standardwerte. Die Anwendung befindet sich zunächst im Environment *development*.

Seit Rails 2.0 ist SQLite 3 das Datenbanksystem, das Entwickler standardmäßig wegen seiner einfachen Handhabung nutzen sollen. Zuvor war es MySQL. Wer dieses System mit der aktuellen Version als Datensilo nutzen will, muss eine Rails-Anwendung mit dem Parameter *-d mysql* erzeugen. Das Framework unterstützt darüber hinaus eine Vielzahl weiterer Datenbanksysteme.

Da *Trainspotr* MySQL verwenden soll, heißt das Abfahrtssignal für die Entwicklung *rails -d mysql trainspotr*. Anschließend lohnt ein Blick in die erzeugten Dateien und Verzeichnisse.

Im Verzeichnis *app* (in *trainspotr*) ist das MVC-Prinzip wiederzuerkennen. In *public* finden Dateien Platz, die Rails direkt an den Browser liefert, ohne sie vorher dem Ruby-Interpreter vorzusetzen – etwa CSS-, Javascript- oder Bilddateien. Die wenigen Konfigurationsdateien befinden sich in *config*,

iX-TRACT

- Ruby on Rails ist ein betriebssystemunabhängiges Web-Framework, das nach dem Model-View-Controller-Prinzip arbeitet.
- Eine Reihe von Konventionen erspart es Entwicklern, komplizierte Konfigurationsoptionen zu pflegen.
- Die Programmierung einer Foto-Gemeinschaft zeigt die wesentlichen Eigenschaften und das Potenzial des Framework.

im Verzeichnis *db* landen später Beschreibungen für Datenbanktabellen. Das *lib*-Verzeichnis ist der richtige Ort für Ruby-Skripte, die Entwickler außerhalb von Modellen, Controllern oder Views schreiben möchten.

Konfigurieren der Verbindung

Die Verbindungs- und Zugangsdaten für die MySQL-Datenbank müssen in *config/database.yml* stehen (siehe Listing 1). Der Inhalt dieser Datei ist in YAML verfasst, einer gern in Rails-Anwendungen verwendeten Markup-Sprache, die es erlaubt, leicht lesbare Konfigurationsdateien oder Test-Fixtures zu notieren. Für jedes Environment kann hier eine eigene Datenbank angegeben werden. Zu beachten ist die Besonderheit der Test-Umgebung, die zwingend eine eigene Datenbank erhalten sollte, falls man die eingebauten Rails-Tests durchführen und Daten eines anderen Environments nicht gefährden will.

Listing 1: config/database.yml

```
development:
  adapter: mysql
  encoding: utf8
  database: trainspotr_development
  username: root
  password:
  host: localhost
test:
  adapter: mysql
  encoding: utf8
  database: trainspotr_test
  username: root
  password:
  host: localhost
production:
  adapter: mysql
  encoding: utf8
  database: trainspotr_production
  username: root
  password:
  host: localhost
```

Listing 2: HTML

```
<!DOCTYPE html
  PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
  <head>
    <title>Trainspotr</title>
    <meta http-equiv="content-type" content="text/html; charset=utf-8">
    <link rel="stylesheet" type="text/css" href="layout.css">
  </head>
  <body>
    <div id="page">
      <div id="header">
       <h1>Trainspotr</h1>
      </div>
      <div id="nav_wrapper">
        <div id="nav">
          (NAV)
        </div>
      </div>
      <div id="main_wrapper">
        <div id="main">
          (MAIN)
        </div>
      </div>
      <div style="clear: both"></div>
      <div id="footer">
        (FOOTER)
      </div>
    </div>
  </body>
</html>
```

Sollten die in Listing 1 angegebenen Datenbanken noch nicht existieren, kann der im Terminal abgesetzte Befehl *rake db:create* die Erzeugung der *development*-Datenbank veranlassen. Um die benötigten Tabellen in dieser Datenbank soll es gleich gehen.

Schon jetzt können Entwickler ihre Rails-Anwendung starten. Den mitgelieferten Webserver Mongrel und damit gleichsam die Anwendung startet *ruby script/server*. Unter http://localhost:3000 lässt sich die Anwendung nun aufrufen. Zum jetzigen Zeitpunkt ist lediglich die Rails-Infoseite zu sehen. Ein Klick auf „About your application’s environment“ sollte keine Fehlermeldung zeigen, sondern Details zu verwendeten Komponenten – das heißt, es besteht eine funktionstüchtige Verbindung zur Datenbank. Ein Blick ins Terminal offenbart schon jetzt Auskünfte über das Geschehen hinter den Kulissen der Anwendung, beispielsweise über die HTTP-Request-Methode, welche Parameter dem Server übergeben wurden, welche Controller und welche Action der Rails-Anwendung dadurch angesprochen und welche Datenbank-Queries erzeugt wurden. Mongrel lässt sich durch Strg+C beenden.

Optisches Layout der Anwendung

Bevor es an die eigentliche Entwicklung der Programmlogik geht, empfiehlt es sich, einen Rahmen, ein Grundlayout mit HTML und CSS zu bauen, das die Ausgaben der Anwendung aufnimmt und Benutzerschnittstellen anbietet. In diesem Fall soll es ein einfaches zweispaltiges Layout sein, wobei die linke Spalte Navigationselemente beinhalten wird. Header- und Footer-Bereich ergänzen den Aufbau (siehe Listing 2).

Für das Layout, das man auf herkömmliche Weise, außerhalb der Rails-Anwendung, gestalten kann, ist es sinnvoll, eine externe CSS-Datei anzulegen. Listing 3 legt zunächst lediglich Wert auf einen Rahmen, weniger auf die optische Gestaltung. Im Bereich *main* wird die Anwendung später den Großteil aller Ausgaben platzieren. In *layout.css* sind hauptsächlich Informationen enthalten, die die Anordnung der einzelnen Container *header*, *nav*, *main* und *footer* betreffen.

Listing 3: layout.css

```
#page { width: 950px; border: 1px solid black; }
#header { border-bottom: 1px solid black; }
#nav_wrapper { width: 197px; float: left; }
#main_wrapper { width: 750px; float: left;
  border-left: 1px solid black; }
#nav, #main { margin: 10px; }
#footer { border-top: 1px solid black; }
```

Nun kann das GUI-Gerüst in die Anwendung integriert werden. Rails erwartet derartige Grundlayouts in *app/views/layouts*. Listing 2 sollte dort als *application.html.erb* liegen. Die Verwendung dieses Dateinamens teilt Rails mit, dass das Layout für die gesamte Anwendung gelten soll. Dies ist eine der eingangs erwähnten Konventionen, die Konfigurationsdaten erspart. Durch die Dateiendung *.erb* „weiß“ Rails, dass diese Datei eingebetteten Ruby-Code enthält, den erst noch das Template-System ERb (Embedded Ruby) interpretieren muss. Dazu gleich mehr.

Für CSS-Dateien gibt es ebenfalls einen festen Platz. Da der Server sie ohne Verarbeitungsschritte direkt an den Browser ausliefert, sollten sie im Verzeichnis *public* und dort im Unterverzeichnis *stylesheets* vorliegen. *application.html.erb* muss nun die Verbindung zu eben dieser CSS-Datei wieder herstellen. Rails übernimmt diese Aufgabe über den Befehl *stylesheet_link_tag*.

Hierbei handelt es sich um einen von unzähligen Helpern, die Rails für die Verwendung in Ansichten, den Views, zur Verfügung stellt und die beispielsweise Grafiken und Javascript-Dateien einbinden oder Formulare und HTML-Tags erzeugen – alles mit Ruby.

Ruby-Code in eine HTML-Datei einzubetten erfolgt durch <% … %>. In *application.html.erb* interpretiert Embedded Ruby diesen Code. Gibt eine Methode, die dort zur Ausführung kommt, etwas aus, bewirkt <%= … %> diese Ausgabe – wie bei *stylesheet_link_tag*, was ein *link*-Element für eine CSS-Datei erzeugt, deren Pfad die von Rails erzeugte Anwendungsstruktur berücksichtigt. Man sollte daher das *link*-Element in *application.html.erb* durch <%= *stylesheet _link_tag 'layout'* %> ersetzen. Die einzubindende CSS-Datei wird als Parameter und ohne Dateiendung hinterlegt.

yield innerhalb des Layouts legt fest, wohin Rails die Ausgaben der

Anwendung schreiben soll. Im vorliegenden Fall ersetze man den Platzhalter *(MAIN)* deshalb durch *<%= yield %>*. Selbstverständlich lassen sich mehrere Stellen innerhalb des Layouts definieren, an denen Daten ausgegeben werden sollen.

Einstieg ins Controlling dank *ActionPack*

Da die Anwendung noch keinen Controller hat, der ihre Ausgaben organisiert und die dafür nötigen Daten besorgt, kann man das Layout noch nicht in Aktion sehen. Ein Controller, dessen Aufgabe es sein soll, die Startseite der Anwendung bereitzustellen, soll das ändern.

Controller sind in Rails Klassen, die von anderen Klassen des Subframeworks *ActionPack* erben. Controller kapseln hauptsächlich die Steuerungslogik der Anwendung. Die Steuerung eines Controllers erfolgt über diverse Aktionen, die innerhalb der Klasse als Methoden implementiert werden. Typischerweise bildet ein Controller CRUD-Operationen (Create, Read, Update, Delete) durch Actions ab, aber dies ist nicht zwingend erforderlich. Der Controller *Home* soll lediglich die Action *index* enthalten, die wiederum einen Willkommenstext zur Anzeige bringt. Diesen Controller und diese Action generiert ein *ruby script/generate controller Home index*.

Rails zeigt die generierten Dateien an. Die Controller-Klasse wurde in *app/controllers/home_controller.rb* erzeugt. Die Bezeichnung der Klasse setzt sich aus dem bei der Generierung angegebenen Namen und dem Zusatz Controller zusammen. Die Klasse besitzt schon die leere Methode *index*, um die es nun gehen soll. In ihr werden nun zwei lokale Variablen erzeugt, *@headline* und *@message*, deren Inhalte beim Aufruf der Action *index* des Controllers zur Anzeige kommen sollen (siehe Listing 4).

Views sind Bestandteil der Präsentationsschicht und beinhalten Teile der

Trainspotr

(NAV) (MAIN)

(FOOTER>

Noch reines HTML. In die durch *(MAIN)* et cetera bezeichneten Bereiche kommt nach und nach mehr Rails (Abb. 1).

Trainspotr

(NAV)

Willkommen bei Trainspotr.

Sie haben Fotos von seltenen Loks? Teilen Sie diese mit anderen Trainspottern!

(FOOTER>

Navigation und Fußzeilen sind noch Demo, im Hauptbereich steht immerhin schon die Begrüßung (Abb. 2).

Anwendungsoberfläche, deren Inhalte der Controller festlegt. Ein View kann beispielsweise HTML und Ruby-Code enthalten, der an die durch *yield* bestimmte Stelle ins Anwendungslayout gesetzt wird. Views liegen standardmäßig im Verzeichnis *app/views* und dort in Unterverzeichnissen, die den Namen des Controllers tragen. Rails nimmt grundsätzlich an, dass zu jeder Action eines Controllers ein View gleichen Namens in diesem Verzeichnis existiert. Deshalb sollten *@headline* und *@message* in app/views/home/index.html.erb eingefügt sein:

```
<h2><%= @headline %></h2>
<p><%= @message %></p>
```

Mongrel ist nun erneut zu starten. Eine Rails-Anwendung ist standardmäßig so konfiguriert, dass eine URL des Musters Host/Controller/Action die Action eines Controllers ausführen kann – bei Bedarf unter Hinzufügen der ID eines Datensatzes. Da es sich bei *index* um die Standard-Action eines Controllers handelt, ist in diesem Fall ihre Angabe nicht nötig, sodass sowohl unter http://localhost:3000/home/index als auch unter http://localhost:3000/home das eben Implementierte zu erreichen ist.

Um diese Ansicht statt der Rails-Infoseite auf der Startseite zu bekommen, die bislang noch unter http://localhost:3000 erscheint, ist ein Eingriff in das eingebaute Routing der Rails-Anwendung erforderlich. Das funktioniert etwa wie *mod_rewrite* bei Apache und erlaubt, URLs auf bestimmte Controller und Actions abzubilden. Die zugehörigen Informationen sollen in *config/routes.rb* liegen. In dieser Datei muss oberhalb des URL-Standard-Mapping die Zeile *map.root :controller => ,home'* stehen, damit die *index*-Action des Home-Controllers zur Startseite wird. Darüber hinaus müssen Entwickler die Rails-Infoseite *public/index.html* entfernen und den Webserver Mongrel wiederum neu starten. Bei Änderungen an *config/routes.rb* ist dies zwingend nötig.

Kernfunktion der Trainspots anlegen

Als Nächstes soll die Anwendung ihre Kernfunktion erhalten – im ersten Schritt ohne benutzerabhängige Features. Es soll möglich sein, eine Zugsichtung anzulegen, zu bearbeiten, zu betrachten und zu löschen. Alle Zugsichtungen sollen in eine eigene Datenbanktabelle, wobei jede Zeile eine Sichtung enthält. Der Zugriff auf Zeilen dieser Datenbanktabelle erfolgt über ein Model.

Jedes Model in Rails ist standardmäßig eine Unterklasse von *ActiveRecord::Base*. Bei Active Record handelt es sich um ein weiteres Subframework. Eigenständig betrachtet ist es ein gut durchdachter objektrelationaler Mapper. Somit enthalten Rails-Models mit ihrer Erzeugung schon alles Nötige für einen unkomplizierten Datenbankzugriff, der weitgehend ohne

Listing 4: Controller

```
class HomeController < ApplicationController
  def index
    @headline = "Willkommen bei Trainspotr."
    @message = "Sie haben Fotos von seltenen Loks? Teilen Sie diese mit anderen Trainspottern!"
  end

end
```

die direkte Nutzung von SQL-Queries auskommt.

Tabellenname als Plural des Bezeichners

Dies trifft auch auf die Erzeugung von Datenbanktabellen zu. Denn das Generieren eines Model impliziert gleichsam eine Migration. Diese ist Ruby-Code, der Datenbanktabellen erzeugen, löschen, ergänzen, mit Daten füllen, leeren und weitere typische Aktionen durchführen kann. Jede Migration besteht aus zwei Methoden. Die eine enthält Schritte zum Durchführen, die andere zum Rückgängigmachen einer Veränderung an der Datenbank. Mit Migrationen existiert eine Art Versionsverwaltung für Datenbanktabellen einer Rails-Anwendung, die während des Entwicklungsprozesses vorteilhaft sein kann und den Bildungsprozess der Datenbankstruktur über den gesamten Entwicklungszeitraum flexibel hält.

Bei der Erzeugung des Model kann man angeben, welche Datenfelder welchen Typs es selbst und damit die dazugehörige Datenbanktabelle enthalten soll. Ein Model-Bezeichner – und damit der Name der Unterklasse von *ActiveRecord::Base* – wird im Singular angegeben. Die Datenbanktabelle selbst erhält als Bezeichnung die Pluralform. Es sind Felder erforderlich, die die Bezeichnung des fotografierten Zuges (train), den Aufnahmeort (location), Datum und Zeit (date) sowie zusätzliche Bemerkungen (notes) aufnehmen sollen:

```
ruby script/generate model Trainspot train:string ⁊
                location:string date:datetime notes:text
```

Rails erzeugt wieder mehrere Dateien, darunter *trainspot.rb* in *app/models*. Dort findet später der Model-Quelltext seinen Platz. Jedes Model erhält seine eigene Datei.

In *db/migrate* befindet sich nun eine Migration. Der automatisch erzeugte Dateiname *001_create_trainspots.rb* weist darauf hin, dass es sich um die erste Migration handelt und mit ihr die Tabelle Trainspots erzeugt wird. Der Dateiinhalt wurde aus den Datenfeldangaben bei der Erzeugung des Model automatisch generiert. Dies kann man mit dem Öffnen der Datei nachvollziehen. Entwickler können beim Erzeugen eines Model auf die Angabe der Datenfelder verzichten und sie direkt in die Migration schreiben (siehe Listing 5).

Rails fügt durch *t.timestamps* der zu erzeugenden Tabelle noch die beiden Felder *created_at* und *updated_at* hinzu, die von Rails selbstständig gepflegt werden und den Zeitpunkt der Erstellung beziehungsweise der jüngsten Bearbeitung eines Datensatzes festhalten. Außerdem wird automatisch das Feld *id* hinzugefügt, wenn die Migration zur Anwendung kommt. Dies erfolgt durch *rake db:migrate*; die Tabelle wird auf Basis der Angaben in der Klassenmethode *up* erzeugt, konkret in der Datenbank, die dem *development*-Environment in *config/database.yml* zugeordnet ist. Entsprechende Ausgaben in der Konsole sollten dies bestätigen.

Das Model Trainspot bringt schon alles mit, was für das Schreiben und Lesen der Tabelle *trainspots* nötig ist. Es fehlen noch Controller mit Actions und Views, die es benutzbar machen.

Der Controller soll Trainspots heißen. Zum Pflegen der Zugsichtungen sind optimalerweise folgende Actions nötig: Anzeigen aller bisherigen Einträge (*index*), Anzeigen eines Eintrags (*show*), Anlegen eines neuen Eintrags (*new*), Speichern eines neuen Eintrags (*create*), Bearbeiten eines bestehenden Eintrags (*edit*), Speichern eines bestehenden Eintrags (*update*) und Löschen eines Eintrags (*destroy*). Die Generierung erfolgt über

```
ruby script/generate controller Trainspots index
show new create edit update destroy.
```

Rails erzeugt daraufhin die Controller-Klasse *TrainspotsController* in *app/controller/trainspots_controller.rb* und die zu den angegebenen Actions gehörenden Views.

REST: Arbeit mit HTTP-Metoden

Mit Rails 2.0 hat sich endgültig REST (Representational State Transfer, die Arbeit mit den HTTP-Methoden *GET*, *POST* et cetera) in Rails fest etabliert. Dies vereinfacht es, einen Controller oder besser ein dahinterstehendes Model als REST-konforme Ressource zu behandeln. Die Actions innerhalb des Controllers werden weiterhin angesprochen, allerdings nicht durch den expliziten Aufruf einer URL, die deren Bezeichner enthält, sondern je nach HTTP-Methode des Requests an den Controller. Die HTTP-Methoden *GET*, *POST*, *PUT* und *DELETE* passen bestens zu den CRUD-Actions eines Rails-Controllers, wobei Actions abseits von CRUD ebenfalls angesprochen werden können.

Um einen Controller RESTful zu machen, genügt ein Eintrag in *config/routes.rb*. Mit *map.resources* gefolgt vom Controller-Bezeichner ist schon alles getan. Für Singleton-Ressourcen steht *map.resource* zur Verfügung. Damit erhalten Entwickler zudem eine Menge sogenannter Named Routes, die sie in Links oder als URL für Formulare nutzen können.

Wenn *map.ressources :trainspots* in *config/routes.rb* hinterlegt ist, kann man mit *rake routes* in der Konsole abfragen, welche Named Routes mit welchen Actions als Ziel zur Verfügung stehen und welche beim Zugriff auf die Ressource verwendete HTTP-Request-Methode welche Action auslöst.

Listing 5

```
class CreateTrainspots < ActiveRecord::Migration
  def self.up
    create_table :trainspots do |t|
      t.string :train
      t.string :location
      t.date :date
      t.text :notes
      t.timestamps
    end
  end
  def self.down
    drop_table :trainspots
  end
end
```

Listing 6: app/views/trainspots/new.html.erb

```
<h2>Neue Zugsichtung anlegen</h2>
<%= error_messages_for :trainspot %>
<% form_for(@trainspot) do |f| %>

  <p>Zug oder Lok<br />
  <%= f.text_field :train %></p>
  <p>Ort der Aufnahme<br />
  <%= f.text_field :location %></p>
  <p>Datum und Uhrzeit<br />
  <%= f.datetime_select :date %></p>
  <p>Bemerkungen<br />
  <%= f.text_area :notes %></p>
  <p><%= f.submit "Speichern" %></p>

<% end %>
<%= link_to '&Uuml;bersicht', trainspots_path %>
```

Listing 7: app/views/trainspots/edit.html.erb

```
<h2>Zugsichtung bearbeiten</h2>
<%= error_messages_for :trainspot %>
<% form_for(@trainspot) do |f| %>
  <p>Zug oder Lok<br />
  <%= f.text_field :train %></p>
  <p>Ort der Aufnahme<br />
  <%= f.text_field :location %></p>
  <p>Datum und Uhrzeit<br />
  <%= f.datetime_select :date %></p>
  <p>Bemerkungen<br />
  <%= f.text_area :notes %></p>
  <p><%= f.submit "&Uuml;bernehmen" %></p>

<% end %>
<%= link_to '&Uuml;bersicht', trainspots_path %>
```

Zur Implementierung der einzelnen Methoden in *TrainspotsController*: Wenn man sich vor Augen führt, dass jede Instanz eines Rails-Model einen Datensatz der gleichnamigen Datenbanktabelle repräsentiert und dass dieses Objekt Methoden zum Lesen, Schreiben und Löschen eines Datensatzes enthält, sind die Actions schnell geschrieben.

Beim Aufruf der Named Route *new_trainspot_url* oder der URL *http://localhost:3000/trainspots/new* kommt die Action *TrainspotsController#new* zum Einsatz. Hier ist lediglich eine leere Model-Instanz erforderlich, die im dazugehörigen View *app/views/trainspots/new.html.erb*, das ein Formular enthalten soll, mit Daten bestückt werden kann. Zu beachten ist hierbei, dass durch die bloße Erzeugung einer Instanz des Model noch keine Änderung an der Datenbank stattfindet.

Listing 9: app/views/trainspots/index.html.erb

```
<h2>Zugsichtungen</h2>
<table>
  <tr>
    <th>Zug oder Lok</th>
    <th>Ort der Aufnahme</th>
    <th>Datum und Zeit</th>
    <th>Bemerkungen</th>
    <th></th>
  </tr>

  <% for trainspot in @trainspots %>
  <tr>
    <td><%= h trainspot.train %></td>
    <td><%= h trainspot.location %></td>
    <td><%= h trainspot.date %></td>
    <td><%= h trainspot.notes %></td>
    <td><%= link_to 'Anzeigen', trainspot %> |
    <%= link_to 'Bearbeiten', edit_trainspot_path(trainspot) %> |
    <%= link_to 'Entfernen', trainspot, :confirm => 'Sind Sie sicher?', :method => :delete %></td>
  </tr>
  <% end %>
 </table>
 <p><%= link_to 'Neue Zugsichtung anlegen', new_trainspot_path %></p>
```

Listing 10

```
class TrainspotsController < ApplicationController

  before_filter :find_trainspot, :only => [:edit, :update, :show, :destroy]
  ...
  private
  def find_trainspot
    @trainspot = Trainspot.find(params[:id])
  end

end
```

Leere Model-Instanz mit initialisierten Daten

Wird dieses Formular gesendet und ist somit ein *POST*-Request an den Controller ergangen, erhält *TrainspotsController#create* diese Formulardaten. Diese Action erzeugt wieder eine leere Model-Instanz – allerdings mit den initialisierten Formulardaten. Erst mit der Methode *Trainspot#save* geht der Versuch einher, die Daten in die Datenbank zu schreiben. Schlägt er fehl – wenn beispielsweise eine notwendige Eingabe fehlt – gibt die Methode *false* zurück. In diesem Falle wird *app/views/trainspots/new/html.erb* erneut angezeigt, allerdings mit den schon eingegebenen Daten und einer Fehlermeldung. Letztere kommt direkt vom Model, erscheint durch *error_messages_for* im View und enthält konkrete Angaben zu Art und Ort des Fehlers.

Ähnliches passiert in den Actions *edit* und *update*, wobei hier der über einen Parameter *ID* an die Action übergebene Datensatz erscheint. Die mächtige Klassenmethode *find* des Model, die auch in den Actions *show* und *destroy* benutzt wird, erhält diesen Parameter und gibt den dazugehörigen Datensatz als Model-Instanz zurück. *TrainspotsController#update* benutzt nicht die Methode *save*, sondern aktualisiert den bestehenden Datensatz durch *update_attributes*. In *TrainspotsController#index* dient *find* dazu, alle bisherigen Zugsichtungen in der lokalen Variable *@trainspots* zu speichern.

Ist das Speichern beziehungsweise Aktualisieren eines Datensatzes in *create* beziehungsweise *update* erfolgreich verlaufen, empfiehlt es sich, einen HTTP-Redirect durchzuführen, beispielsweise auf die Seite aller bisherigen Einträge. Gleiches gilt für die Action *destroy*. Dieser Redirect verhindert, dass der *POST*-, *PUT*- oder *DELETE*-Request auf die Ressource durch Aktualisieren der Webseite erneut durchgeführt wird.

Das schon standardmäßig existierende Objekt *flash* ermöglicht es, eine Meldung an den Benutzer zu hinterlegen, die diesen Redirect gleichsam „überlebt“ und innerhalb des Weiterleitungsziels zur Anzeige kommen kann. Da dies Standard in Rails-Anwendungen ist, empfiehlt es sich, im Layout eine Stelle zu definieren, die diese Meldung aufnehmen soll. Mit *<%= flash[:notice] %>* oberhalb des *yield*-Befehls in *app/views/layouts/application.html.erb* lässt sich das umsetzen.

Form-Element automatisch erstellt

Die Views *new* und *edit* zeigen ein Formular zur Dateneingabe. Die Daten entstammen einer Model-Instanz. Mit dem Helper *form_for* und dieser Instanz als Parameter erstellt Rails automatisch das benötigte *form*-Element inklusive aller benötigten Attribute für ein reibungsloses Zusammenwirken mit dem Controller.

Und noch mehr: *form_for* kann ein Block übergeben werden, innerhalb dessen ein Form-Helper-Objekt als Blockvariable zur Verfügung steht, das über Methoden verfügt, mit denen sich die einzelnen Formularelemente erzeugen lassen. Auch diese werden dank *form_for* mit allen nötigen Attributen

Anlegen eines Fotos samt Kommentar; noch ist die Navigation „leer“ (Abb. 3).

Listing 8: app/views/trainspots/show.html.erb

```
<h2>Zugsichtung <%=h @trainspot.train %></h2>
<p><b>Ort der Aufnahme:</b><br />
<%= h @trainspot.location %></p>
<p><b>Datum und Uhrzeit:</b><br />
<%= h @trainspot.date %></p>
<p><b>Bemerkungen:</b><br />
<%= h @trainspot.notes %></p>
<p><%= link_to 'Bearbeiten', edit_trainspot_path(@trainspot) %> |
<%= link_to '&Uuml;bersicht', trainspots_path %></p>
```

Listing 11: app/views /trainspots/_form.html.erb

```
<p>Zug oder Lok<br />
<%= f.text_field :train %></p>
<p>Ort der Aufnahme<br />
<%= f.text_field :location %></p>
<p>Datum und Uhrzeit<br />
<%= f.datetime_select :date %></p>
<p>Bemerkungen<br />
<%= f.text_area :notes %></p>
```

versorgt. Hier sind *text_field*, *text_area* und *datetime_select* (mehrere Auswahlfelder zur Datums- und Zeiteingabe) erforderlich; dazu kommt ein Submit-Button. Unterhalb des Formulars verweist ein Link durch die Named Route *trainspots_path* auf die Übersicht, die Action *TrainspotController#index* (siehe Listing 6 und 7).

TrainspotsController#show (siehe Listing 8) funktioniert ähnlich wie die beiden bisherigen Views, nur dass es hier ausschließlich ums Anzeigen geht. Der Helper *h* bereitet alle anzuzeigenden Daten HTML-gerecht auf, zudem verhindert er Cross-Site Scripting durch das Entschärfen von Javascript-Anweisungen.

Die Übersicht aller Zugsichtungen besteht aus einer Tabelle. Mit *@trainspots* steht ein Array zur Verfügung, dessen Elemente Model-Instanzen sind. Eine Iteration erstellt für jede Zugsichtung eine Tabellenzeile. In der rechten Spalte befinden sich jeweils Links, mit denen ein Datensatz bearbeitet, betrachtet oder gelöscht werden kann (siehe Listing 9). Der Rails-Helper *link_to* ermöglicht durch den Parameter *confirm*, eine besonders gefährliche Aktion durch eine Nachfrage abzusichern. Er erzeugt den nötigen Javascript-Code für eine Bestätigungsbox.

Views für die Actions *create*, *update* und *destroy* sind nicht nötig, da diese lediglich eine Operation ausführen. Die Dateien kann man bedenkenlos löschen.

Don't Repeat Yourself

Im momentanen Programmcode gibt es mehrere Stellen, an denen sich Code wiederholt. Der erste Teil dieses Tutorials soll damit beschlossen werden, zwei Features vorzustellen, die zeigen, dass Rails gut dabei unterstützt, das DRY-Prinzip umzusetzen.

In *TrainspotsController* befindet sich in den Actions *edit*, *update*, *show* und *destroy* dieselbe Zeile: *@trainspot = Trainspot.find(params[:id])*. Mit Filtern können Entwickler separate Methoden schreiben, die vor oder nach dem Ausführen bestimmter Actions zur Ausführung kommen. Hier geht es um *before_filter*. Listing 10 erhält als Parameter die auszuführende Methode und einen Array der Actions, bei denen der Filter greifen soll. Zu streichen ist deshalb die eben genannte Zeile aus den betreffenden Actions. Da die Methoden *show* und *edit* nun ohne Inhalt sind, kann man sie gänzlich aus dem Controller streichen. Rails führt in diesem Fall nur noch den Filter aus und lädt den zugehörigen View. Der Controller ist wie in Listing 10 zu sehen zu ergänzen.

Eine weitere Stelle, an denen Code mehrfach auftritt, lässt sich in den Trainspots-Views *new.html.erb* und *edit.html.erb* finden. Das Formular ist in beiden Fällen weitgehend identisch. Mit Partials lassen sich gleiche Teile von Views auslagern und wiederverwenden. Partials sind Views, deren Dateinamen mit einem Underscore beginnen – eine weitere Rails-Konvention. In app/views/trainspots/_form.html.erb sind die identischen Formularelemente zu sehen (Listing 11).

In *new.html.erb* und *edit.html.erb* kann dieser Teil nun jeweils durch Rails' *render*-Befehl ersetzt werden. Hier steht der Name des Partials – ohne Underscore. Zudem muss das Formular-Objekt als lokale Variable an das Partial übergeben werden, damit dies es verwenden kann: *<%= render :partial => ‚form', :locals => {:f => f} %>*.

Tutorialinhalt

Teil I:	**Einrichten der Umgebung, Aufbau des Grundlayouts der Website sowie Model, Controller und View für das Anlegen und Bearbeiten von Loksichtungen**
Teil II:	Datei-Upload, Thumbnail-Erzeugung, Anlegen eines geschützten Bereichs mit Registrierung, dynamische Navigation, Geodaten mit Google Maps
Teil III:	Startseite mit Fotos aus dem Datenbestand und Ajaxifizieren der Oberfläche. Hinweise zum Deployment

Fazit

Bislang lassen sich in *Trainspotr* zwar Zugsichtungen hinterlegen, allerdings fehlt noch das Wichtigste: die Fotos. Um das Hochladen und das automatische Anfertigen von Thumbnails soll es im nächsten Teil gehen. Außerdem, wie Geodaten zu diesen Fotos hinterlegt und mit Google Maps angezeigt werden können. Es entsteht zudem ein geschützter Benutzerbereich und eine dynamische Navigationsleiste für die linke Seite des Layouts.

Dabei wird es noch mehr um Migrations und Routing gehen, das Verwenden von Validatoren und Assoziationen. Außerdem um das Einbinden und Nutzen von Plug-ins sowie um einige Werkzeuge, die Ruby on Rails mitbringt. Der Quelltext zu *Trainspotr* in seiner jetzigen Form steht auf dem FTP-Server der *iX* und unter www.trainspotr.de zur Verfügung. Dort kann man die Anwendung außerdem ausprobieren. (hb)

DENNY CARL

ist seit 2001 selbstständiger Webdesigner und -entwickler in Berlin.





Onlinequellen

Rails	
Ruby on Rails – offizielle Website	www.rubyonrails.org
Ruby on Rails (deutsche Seite)	www.rubyonrails.de
Rails-Dokumentation	api.rubyonrails.org
Railscasts – Screencasts zu Rails	www.railscasts.com
Rails Usergroup Deutschland	www.rubyonrails-ug.de/
Editoren und IDEs	
Textmate (Mac OS X)	macromates.com/
E-TextEditor (Windows)	www.e-texteditor.com/
Netbeans (OS-unabhängig)	www.netbeans.org/
Aptana/RadRails (OS-unabhängig)	www.aptana.com/
3rdRail (Windows, Mac OS X, Linux)	www.codegear.com/products/3rdrail
Heroku online (OS-unabhängig)	heroku.com/



MySQL via SSH-Tunnel nutzen

Licht am Ende

Alexander Mas, Steffan Schiewe, Bernhard Wellhöfer

Oft akzeptieren Datenbanken aus Sicherheitsgründen Verbindungen nur von lokalen Clients, was die Arbeit aus der Ferne übermäßig erschwert. Ein automatisch aufgebauter SSH-Tunnel bietet in Zusammenarbeit mit *xinetd* und *netcat* allen Clients sicheren Zugriff von entfernten Rechnern.

Unternehmen verwenden häufig Webserver mit zugehöriger Datenbank bei einem externen Provider. Aus Sicherheitsgründen sind dort nur die zwingend notwendigen Ports für Protokolle wie HTTP (80), HTTPS (443) und SSH (22) von außen zugänglich. Außerdem verbinden sich alle nur lokal verwendeten Dienste, zum Beispiel die Datenbank, mit dem virtuellen Interface *localhost*. Damit entfällt der direkte Zugriff von außen auf diese Dienste. Insbesondere die Nutzung der auf dem externen Server laufenden Datenbank ist aus dem Unternehmen heraus nicht möglich.

Einen Weg zur Verwaltung und zum Zugriff auf die Datenbank öffnen Webwerkzeuge wie *PHPMyAdmin*. Neben der üblichen Anmeldung mit Login und Passwort bringt eine HTTP-Authentifizierung zusätzliche Sicherheit. Oft reicht aber dieses Vorgehen für die tägliche Arbeit nicht aus. Viele Funktionen bieten nur Anwendungen mit direkter Verbindung zur Datenbank. Beispiele dafür sind Applikationen wie der MySQL Query Browser, automatische Backups per *mysqldump*, statistische Analysen mit SPSS direkt auf den Daten sowie Skripte für Datamining oder zum Erstellen von Reports.

Dieser Artikel zeigt Schritt für Schritt eine Lösung für das geschilderte Dilemma. Sie verwendet einen lokalen „Port-Proxy-Server“, der als allgemeiner Dienst die Kommunikation mit der Datenbank des entfernten Servers über eine sichere SSH-Verbindung kapselt und zur Verfügung stellt. Zum Aufbau eines SSH-Tunnels verwendet man den folgenden Befehl:

```
ssh -l login-name -N \
  -L [bind_address:]port:host:hostport remoteServer
```

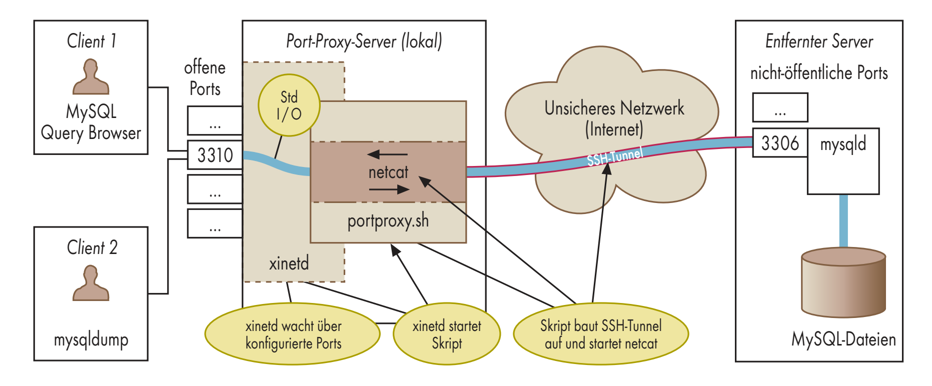
Der Parameter *-l* definiert den Nutzernamen, für den auf den entfernten Server die Authentifizierung stattfindet. *-L* legt fest, dass der lokale *port*, optional gekoppelt an eine IP-Adresse (*bind_ address*), auf dem entfernten Rechner *remoteServer* an die IP-Adresse *host* und den Port *hostport* weitergeleitet wird. Statt IP-Adressen lassen sich Namen angeben; allerdings erfolgt die Auflösung von *host* auf dem Zielrechner. *-N* verhindert das Starten der Login-Shell. Beispielhaft hier der Aufruf, um einen Tunnel zur MySQL-Datenbank auf dem entfernten Server (gebunden dort an *localhost:3306*) aufzubauen:

```
ssh -l user-remote -N \
  -L 12345:localhost:3306 remoteServer
```

Ein *mysql*-Client lässt sich nun etwa so via *ssh* mit der entfernten Datenbank *db* verbinden:

```
mysql --port=12345 -h 127.0.0.1 \
  --user=dbUser --password=dbPasswd db
```

Mit der Angabe *-h 127.0.0.1* erzwingt man die Nutzung einer TCP-Verbindung über den angegebenen Port – üblicherweise verwendet *mysql* lokal



Lokale Datenbankprogramme verbinden sich mit Port 3310, den der *xinetd* mithilfe von *netcat* und einem SSH-Tunnel an die entfernte Datenbank weiterleitet (Abb. 1).

immer einen Socket und ignoriert den Port-Parameter. Die Werte von *--user* und *--password* dienen zur Authentifizierung mit der Datenbank.

Schlüssel vereinfachen SSH-Anmeldung

Beim erstmaligen Aufbau einer SSH-Verbindung für diesen Benutzer zum entfernten Server muss der Anwender dessen SSH-Fingerprint akzeptieren und in der Regel sein Passwort zur Anmeldung eingeben. Um diese Eingabe zu vermeiden und das automatisierte Ausführen von Skripten zu erleichtern, verwendet man ein Schlüsselpaar zur Authentifizierung. Auf die Details geht dieser Text nicht ein, Näheres dazu erläutern unter anderem Barret und seine Kollegen [1].

Nach dem erfolgreichen Einrichten der Authentifizierung per Schlüssel sollte als Test das Kommando

```
ssh -l user-remote remoteServer hostname
```

den Befehl *hostname* auf dem entfernten Server ohne weitere Rückfrage ausführen und den Rechnernamen als Resultat ausgeben.

Mit *xinetd* und dem als *nc* aufgerufenen *netcat* lässt sich der Aufbau des SSH-Tunnels automatisieren und sein lokaler Port für Tools wie den MySQL Query Browser oder *mysqldump* einfach bereitstellen. Beide Kommandos stehen unter Linux in jeder Distribution zur Verfügung und können beispielsweise bei Debian als Root mit dem Befehl *apt-get install nc xinetd* installiert werden.

Als einfacher Funktionstest kommt der Echo-Dienst zum Einsatz, der alle eingehenden Daten liest und sie sofort unverändert zurücksendet. Dazu setzt man in der Datei */etc/xinetd.d/echo* im Abschnitt für die TCP-Version den Wert *disable* auf *no*. Abschließend veranlasst */etc/init.d/xinetd reload* den Daemon zum erneuten Einlesen der Konfigurationsdateien.

Für die meisten bekannten Netzdienste ordnet */etc/services* den Portnummern sprechende Namen zu. Für den Echo-Dienst finden sich dort die Portnummer 7 und „echo“ als Name. *netstat -an| grep :7* zeigt, ob *xinetd* den Port und damit den Echo-Dienst bereitstellt. Ist dies nicht der Fall, sollten die üblichen Logdateien in */var/log* Aufschluss über die Ursache geben.

Listing 1: Dienstkonfiguration für *xinetd*

```
# default: on
service server-portproxy-3310
{
   port            = 3310
   type            = UNLISTED
   socket_type     = stream
   wait            = no
   user            = user_local
   server          = /opt/portproxy.sh
   server_args     = -t remote_server 3306 user_remote
   log_on_success  += USERID PID HOST EXIT DURATION
   log_on_failure  += USERID HOST ATTEMPT
   disable         = no
   log_type        = FILE /tmp/portproxy.xinetd.log
}
```

Kopierer für den IP-Verkehr

In der einfachsten Verwendung *nc host port* öffnet *netcat* eine TCP-Verbindung zum angegeben Zielrechner und -port. Anschließend kopiert es alle Daten aus der Standard-Eingabe in die geöffnete Netzverbindung und umgekehrt alles von dort auf die Standard-Ausgabe. Mit *nc localServerName echo* lässt

Listing 2: Skript für den automatischen Verbindungsaufbau

```
#!/bin/bash
# Usage: $0 dbServerHost dbServerPort userNameForTunnel

# prepare logging
LOGFILE=/tmp/`basename $0 .sh`.log

function log() {
		echo $$: $@ >>$LOGFILE
}

log start $0 at `date` with arguments -"$@"-

# find a free port, assign free port to $port
function getFreePort() {
	while true
	do
		port=$RANDOM
		[ $port -lt 1025 ] && continue
		netstat -an | fgrep -q ':'$port || break
	done
}

# the function does the work (see comments inside), arguments:
#    $1 the remote host
#    $2 the remote port
#    $3 the remote ssh user
function doWork() {
		# get free local port for the ssh tunnel
		getFreePort
		log free port is $port

		# build tunnel to remote host
		log start tunnel to remote host $1 to port localhost:$2 for user $3
		ssh -l $3 -C -L $port:localhost:$2 -N $1 >> $LOGFILE 2>&1 &

		# wait max up to 20 seconds for the tunnel to start
		s=1
		while ! netstat -an | grep -q ':'$port
		do
			log waiting for ssh tunnel -$s-
			sleep 1
			s=$(($s + 1))

			if [ $s -gt 20 ]
			then
				log unable to start ssh tunnel
				exit 1
			fi
		done
		log tunnel built

		# start I/O copying
		log start nc copy program for stdin/stdout and localhost:$port
		nc localhost $port 2>>$LOGFILE

		# kill background tunnel
		log killing ssh tunnel
		kill %1
}

# test arguments: $0 dbServerHost dbServerPort userNameForTunnel
if [ $# -ne 3 ]
then
		log `basename $0` was called with an illegal argument list: "$@"
		exit 1
fi

# do the work
doWork $1 $2 $3

log end of $0 at `date`
exit 0
```

sich folglich der von *xinetd* angebotene Echo-Dienst testen.

Mit *xinetd*, *netcat* und dem SSH-Tunnel stehen alle Komponenten für den Aufbau des „Port Proxy Servers“ bereit. Abbildung 1 zeigt schematisch den Aufbau und die Funktionsweise.

Pro entfernte Datenbank existiert auf dem „Port-Proxy-Server“ ein Port als Stellvertreter, den *xinetd* bewacht. Verbindet sich ein lokaler Datenbank-Client mit diesem Port, startet der Daemon ein Shell-Skript, das einen SSH-Tunnel zur entfernten Datenbank öffnet und *netcat* zum Kopieren der Daten von dem lokalen Client zur Datenbank und zurück startet.

Listing 1 zeigt beispielhaft die zugehörige *xinetd*-Konfigurationsdatei, die in */etc/xinetd.d* liegen muss. Sie legt unter anderem den lokalen Pfad zum erwähnten Shell-Skript und dessen Parameter (*server* und *server_args*) sowie Logging-Einstellungen fest. Eine genaue Erklärung der weiteren Zeilen liefern die zugehörigen Manual-Seiten (*man xinetd.conf*). Damit unterschiedliche Proxy-Verbindungen zu mehreren Servern möglich sind, kann diese Konfiguration dupliziert und mit angepasstem Port und Skriptparametern gespeichert werden. Wie zuvor muss */etc/init.d/xinetd reload* den *xinetd* zum erneuten Lesen der Konfiguration veranlassen.

Listing 2 zeigt Auszüge aus dem von *xinetd* gestarteten Shell-Skript, das den SSH-Tunnel und *netcat* aktiviert. Die vollständige Fassung steht auf dem *iX*-Listingserver bereit. Das Skript sucht zunächst nach einem freien Port größer als 1024, der anschließend die lokale Seite des SSH-Tunnels bildet. Da dieser im Hintergrund läuft, wartet das Skript bis zu seinem erfolgreichen Start. Mit *netcat* kopiert es dann alle ein- und ausgehenden Daten zwischen dem lokalen Client und dem SSH-Tunnel. Fügt man noch Fehlerprüfungen und Logging-Funktionen hinzu, entsteht das komplette Shell-Skript. So lässt sich nun zum Beispiel die entfernte Datenbank sichern:

```
mysqldump --port=3310 -h 127.0.0.1 \
  --user=dbUser --password=dbPasswd db \ ↵
                                    > backup.sql
```

Ist der „Port Proxy Server“ eingerichtet, bietet er von jedem Rechner im lokalen Netz Zugriff auf die entfernten Datenbanken.

Fazit

Wenn es keinen direkten Zugriff auf bestimmte Dienste eines entfernten Servers gibt, bietet das hier vorgestellte Skript eine einfache und sichere Lösung, diese aus dem lokalen Netz zu verwenden. Im Fall eines Datenbankdienstes auf dem entfernten Server ist man dadurch in der Lage, administrative Aufgaben zu erledigen oder automatisierte Skripte auszuführen, die eine direkte Verbindung zur Datenbank benötigen. Mit kleineren Anpassungen lässt sich dieses Verfahren auch für andere Dienste einsetzen (ck).

ALEXANDER MAS

ist freiberuflich tätig bei der Gaia AG und Student im Informatik-Masterstudiengang der Hochschule für angewandte Wissenschaften Hamburg.

STEFFAN SCHIEWE

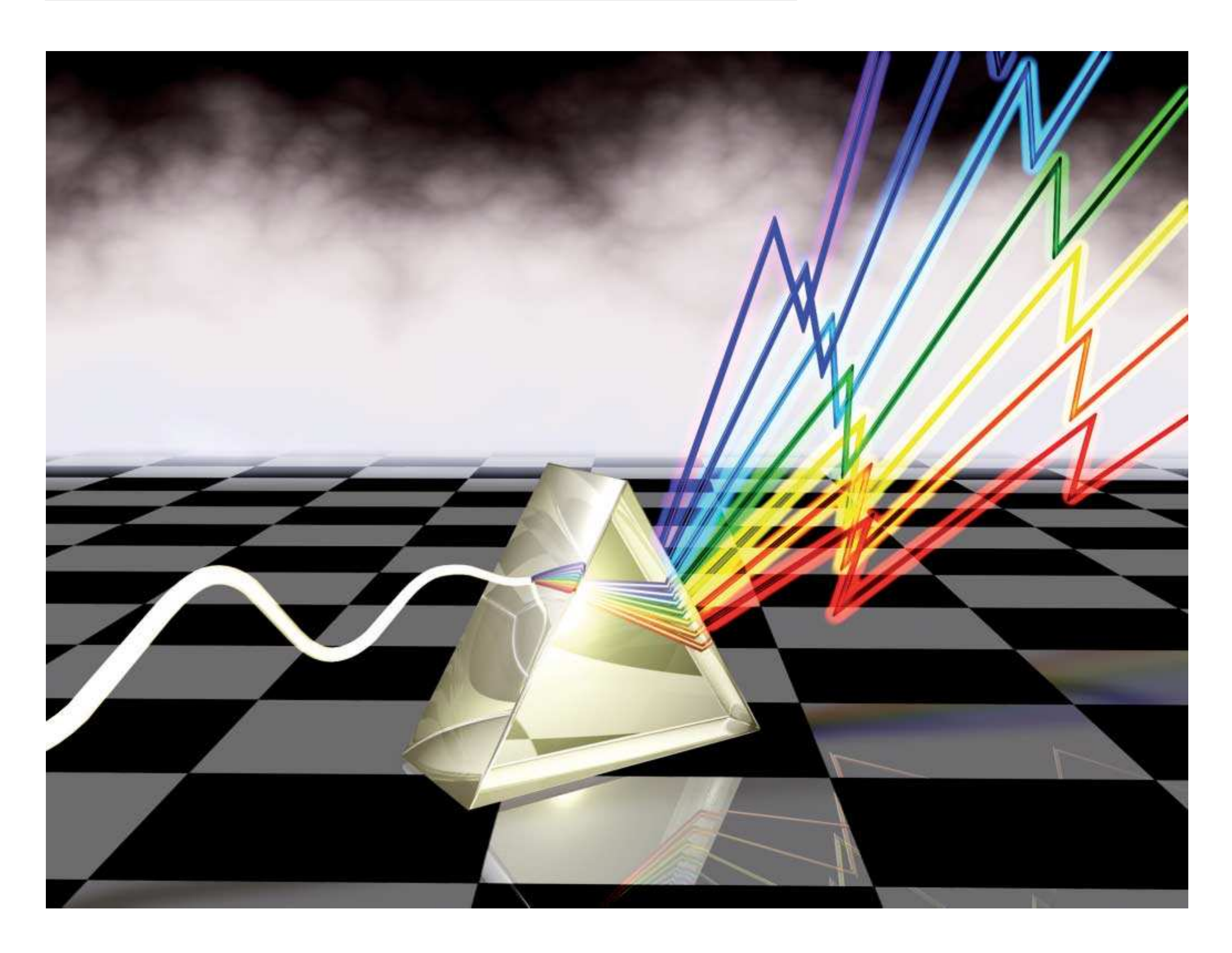
ist Geschäftsführer der YOOlabs GmbH und beschäftigt sich mit der Konzeption und Realisierung professioneller Webauftritte.

BERNHARD WELLHÖFER

heißt nun nicht mehr Kühl, lebt in der brückenreichsten Stadt Europas und fährt leider nicht mehr Ski in der Ramsau.

Literatur

[1] Daniel J. Barret, Richard E. Silvermann, Robert G. Byrnes; SSH, The Secure Shell. The Definitive Guide; O’Reilly Media; Sebastopol 2005; ISBN 0-596-00895-3



Open-Source-Compiler für Actionscript

Frei eingeblendet

Uwe Seimet

Adobes Flash Player ist ein weit verbreitetes Browser-Plug-in. Mit seiner Hilfe lassen sich nicht nur Webanwendungen mit Animationen oder Video-Streaming realisieren, sondern in Verbindung mit einem geeigneten Server auch Client/Server-Anwendungen. Dazu kommen neben Softwarepaketen von Adobe freie Werkzeuge infrage.

Laut einer Statistik von Adobe ist auf fast 99 Prozent aller PCs ein Flash-Player-Plug-in installiert, davon zu einem überwiegenden Teil die aktuelle Version 9 (siehe „Onlinequellen“ [a] – die Quellen finden sich im Web unter „*iX*-Link“). Von einem solch hohen Verbreitungsgrad sind andere bekannte Browser-Plug-ins – insbesondere Java und der Windows Media Player – ein ganzes Stück entfernt. Anwendungen für den Flash Player erstellen Programmierer in der Regel mit der kommerziellen IDE Flash CS3 Professional, die nur für Windows und Mac OS X verfügbar ist. Flash CS3 erlaubt sowohl die Gestaltung der grafischen Elemente einer Webanwendung als auch die Programmierung clientseitiger Logik in der objektorientierten Programmiersprache Actionscript, die wie Javascript an den ECMAScript-Standard angelehnt ist.

Die Daten einer Flash-Anwendung sind in einer vom Flash Player ausführbaren SWF-Datei eingebettet, wobei SWF je nach Lesart für Small Web Format oder Shockwave Flash steht. SWF-Dateien sind plattformunabhängig und, sofern keine zusätzlichen Daten benötigt werden, kann das Browser-Plug-in sie ausführen, ohne weitere Ressourcen im Netz in Anspruch zu nehmen. Dies trifft auf viele mit Flash realisierte Animationen zu. Etwas komplizierter ist es bei Anwendungen aus dem Multimedia-Bereich. Zwar lassen sich auch Videos in eine SWF-Datei integrieren, aber sinnvoll ist dies ab einem gewissen Datenvolumen nicht mehr, da das Plug-in zunächst die gesamte Anwendung mit allen Daten herunterladen muss, bevor

es ein Video starten kann. Eine bessere Lösung ist der progressive Download, bei dem der Player die Anfangssequenz eines Videos schon abspielt, während er fehlende Daten noch im Hintergrund lädt. Progressive Downloads lassen sich mit einem handelsüblichen Webserver realisieren, erlauben ein Umherspringen in einem Video jedoch nur innerhalb der bereits vom Plug-in geladenen Daten.

Im Idealfall erfolgt die Übertragung von Audio/Videodaten durch einen Streaming-Server, der mit dem Flash Player in ständigem Kontakt steht. Dieser Server übermittelt die vom Client benötigten Daten nahezu in Echtzeit und ermöglicht daher auch die Übertragung von Live-Veranstaltungen. Innerhalb eines vorproduzierten Videos kann der Anwender ohne nennenswerte Verzögerungen vor- und zurückspulen. Professionelle Streaming-Server verstehen sich aber nicht nur auf die Übermittlung reiner Video- und Audio-Daten. Grundsätzlich lassen sich beliebige Daten zwischen Server und Flash-Plug-in austauschen, somit auch Informationen über Methoden-Aufrufe. Damit kann der Flash Player Server-Funktionen abrufen oder umgekehrt der Server Funktionen des Players steuern. Dabei kommt ein proprietäres Client-Server-Protokoll zum Einsatz, das aber Open-Source-Anwendungen aus dem Flash-Umfeld ebenfalls verstehen [b].

Eine einfache Server-Anwendung in Actionscript: Sobald der Server eine Client-Verbindung akzeptiert, führt er die nächsten Anweisungen aus.

Listing 1: *main.asc*

```
application.onConnect = function(client) {
    // Eingehende Verbindung immer akzeptieren
    this.acceptConnection(client);
    // Debug-Ausgabe ins Server-Logfile und auf die Webkonsole
    trace("Client connection accepted from IP " + client.ip +
          " at " + new Date());
    // Die Methode 'echo' erwartet einen String als Parameter und ruft
    // damit die Methode 'say' des Clients auf
    client.echo = function(str) {
        trace("Client said '" + str + "'");
        this.call("say", null, "Server echoes: " + str);
    }
    // Sendet durch Aufruf der Client-Methode 'setServerTime'
    // die aktuelle Server-Zeit an den Client
    trace("Sending current server time to client");
    client.call("setServerTime", null, new Date());
}
```

Installation des FMS unter Linux

Handelt es sich bei der Zielplattform nicht um eine von Adobe offiziell unterstützte Linux-Distribution, lässt sich oft dennoch eine lauffähige Installation des FMS2 oder FMS3 einrichten. Hierzu deaktiviert man zunächst im Installations-Script *installFMS* durch Auskommentieren der *exit*-Anweisungen in den Zeilen 36, 45, 60 und 75 die plattformspezifischen Sicherheitsabfragen und führt anschließend die reguläre Installation durch. Nun überprüft im Unterverzeichnis *fms* des Installationspfads der Aufruf von

```
ldd fmsadmin fmscore
```

ob alle benötigten Shared Libraries in den erforderlichen Versionen vorhanden sind. Dies ist nicht immer der Fall, da die Versionsnummern der relevanten Bibliotheken von denen bei Red Hat abweichen können. Abhilfe schafft das Anlegen symbolischer Links für die fehlenden Dateien, möglichst in einem separaten Verzeichnis.

Auf 64-Bit-Systemen muss der Kernel Anwendungen im 32-Bit-Kompatibilitätsmodus ausführen können und die Links für fehlende Bibliotheken müssen sich auf die 32-Bit-Bibliotheken beziehen. Das Hinzufügen des Verzeichnisses mit den Links sowie des Verzeichnisses *fms* zur Umgebungsvariablen *LD_LIBRARY_PATH* informiert den Laufzeit-Linker über das Vorhandensein der neuen Libraries. Anschließend lassen sich der Flash Media Server sowie der Administrationsserver mit

```
./fmsmgr server fms start
./fmsmgr adminserver start
```

auch auf einer Linux-Distribution wie Suse 9.3 und neuer oder Gentoo starten.

Flash Media Server und Alternativen

Im Gegensatz zum frei verfügbaren Flash Player handelt es sich bei den Flash-kompatiblen Servern überwiegend um kommerzielle Produkte. Adobe bietet den Flash Media Server 3 (FMS 3) für Windows und Linux seit Anfang 2008 als Nachfolger des FMS 2 beziehungsweise des Flash Communication Server in zwei Versionen an, von denen lediglich die teurere Variante, der Flash Media Interactive Server, eigene serverseitige Anwendungen ausführen kann [c]. Offiziell unterstützte Plattformen für den FMS sind Windows Server 2003 und Red Hat Linux 4. Die Installation verläuft jedoch auch auf Windows XP Professional erfolgreich, und durch kleine Manipulationen bei der Installation lassen sich außer Red Hat auch andere Linux-Distributionen einsetzen (siehe Kasten zur Installation).

Zu Adobes Server existieren alternative Produkte wie der Wowza Media Server [d], der auch für Debian Linux, Mac OS X und Solaris erhältlich ist. Im nichtkommerziellen Umfeld tummelt sich der plattformunabhängige Server Red5, der sich allerdings noch im Beta-Stadium befindet [e]. Adobes FMS3 und der Wowza-Server sind jeweils als kostenlose Evaluierungs-Ausführung für maximal zehn gleichzeitige Client-Verbindungen verfügbar. Mit diesen Versionen lässt sich der komplette Funktionsumfang für Entwicklungszwecke nutzen.

Anders als bei Adobes FMS ist die Programmiersprache des Wowza-Servers und von Red5 nicht Actionscript, sondern Java. Eine einfache Übernahme bereits vorhandener serverseitiger Actionscript-Anwendungen für den FMS ist bei einem Wechsel des Server-Anbieters daher nicht machbar. Der Einsatz von Java statt Actionscript auf der

iX-TRACT

- Die Kommunikation von in Actionscript programmierten Client/Server-Anwendungen erfolgt über ein proprietäres Middleware-Protokoll, das auch einige Open-Source-Compiler kennen.
- Mit einigen Einschränkungen unterstützen die freien Compiler MTASC und haXe die Entwicklung von Flash-Player-Anwendungen auch ohne die Flash IDE.
- Das Fehlen einer freien Flash-ähnlichen IDE erschwert zwar die Entwicklung von Anwendungen mit grafischen Elementen auf der Basis freier Werkzeuge, dafür lässt sich andererseits mit haXe eine Brücke zwischen Actionscript und Javascript schlagen.

Server-Seite kann aber auch von Vorteil sein, bietet sich doch die Möglichkeit zur Wiederverwendung von bereits vorhandenem Java-Code und zur Nutzung der umfangreichen Java-APIs.

Konzepte müssen verstanden sein

Bei Server-Side Actionscript (SSAS) für die Programmierung des FMS handelt es sich um eine recht alte Ausprägung von Actionscript, die aus Javascript 1.5 hervorgegangen ist. Neben Adobes Website ist insbesondere Brian Lessers Buch [1] als Informationsquelle zur Programmierung in SSAS zu empfehlen. Zur Einrichtung einer serverseitigen Anwendung für den FMS genügt es, auf dem Server im Verzeichnis *applications* ein neues Unterverzeichnis mit dem Namen der Anwendung anzulegen. Darin wird eine Textdatei namens *main.asc* platziert, die Anweisungen in SSAS enthält. Bei Bedarf lassen sich zusätzliche SSAS-Klassen in weiteren Dateien hinterlegen. Sobald sich ein Client mit der Server-Anwendung verbindet, startet der Server *main.asc* und führt die darin befindlichen Anweisungen aus. Die Kontrolle des Servers und einzelner Anwendungen erfolgt durch die als Webanwendung verfügbare Administrationskonsole, die Bestandteil der FMS-Distribution ist.

Die API des Flash Media Servers ist nicht nur darauf ausgelegt, Audio- und Video-Daten effizient als Stream zu übertragen. Mit einem gegenüber anderen Middleware-Techniken vergleichsweise geringen initialen Programmieraufwand lassen sich Verbindungen zu Flash-Clients aufbauen und wechselseitig Methoden aufrufen. Auch wenn die FMS-API erste Schritte bei der Nutzung der serverseitigen Flash-Technik gut unterstützt, darf dies nicht darüber hinwegtäuschen, dass die Entwicklung robuster Anwendungen auch hier ein tieferes Verständnis der zugrunde liegenden Konzepte erfordert.

Als Einstieg in die Programmierung des FMS zeigt Listing 1 eine einfache Anwendung in SSAS, aus der einige Grundregeln für die Client/Server-Kommunikation mit Flash und Actionscript hervorgehen. Der Server arbeitet ereignisorientiert und führt beim Eintreten bestimmter Events die zugeordneten Methoden aus. So ruft er *onConnect()* auf, sobald ein Client versucht, eine Verbindung mit einer Serveranwendung aufzunehmen. Ob sie diese Verbindung zulässt, entscheidet der Server anhand der vom Client übermittelten Daten. Verbindungen zwischen dem Flash-Server und dem Browser-Plug-in sind persistent und werden automatisch geschlossen, sobald der Anwender die Webseite mit der laufenden Flash-Player-Anwendung verlässt.

In Listing 1 bestätigt *acceptConnection()* den Verbindungsaufbau ohne weitere Prüfung eventueller Parameter und *trace* schreibt eine Information ins Logfile. Für das Client-Objekt, dessen Referenz die Server-Anwendung beim Verbindungsaufbau erhalten hat, lassen sich nun serverseitige Methoden definieren, die der Flash Player anschließend aufrufen kann. Als einfaches Beispiel dient die Definition der Methode *echo()*, die eine Zeichenkette als Argument erhält. *echo()* tut nichts weiter, als den Aufruf serverseitig mit einer *trace*-Anweisung zu protokollieren und anschließend die Methode *say()* des Clients mit der soeben erhaltenen Zeichenkette als Parameter aufzurufen. Am Ende der Initialisierung schickt der Server durch den Aufruf der Client-Methode *setServerTime()* die aktuelle Server-Zeit an den neu registrierten Client und steht nun für die weitere Kommunikation bereit.

Bis auf die Verfügbarkeit der *trace*-Anweisung, mit der sich zur Kontrolle des Programmflusses Debug-Information in der Webkonsole anzeigen beziehungsweise in Logdateien schreiben lässt, bietet der FMS leider keine Debugging-Hilfen an, sodass sich das Testen einer SSAS-Anwendung und die Fehlersuche umständlich gestalten. Eine IDE zur besseren Unterstützung der Entwicklung in SSAS stellt Adobe nicht bereit. Insbesondere fehlt ein Debugger auf Quelltext-Ebene, wie man ihn für die Client-Seite in der Flash-IDE findet. Die Entwicklung größerer serverseitiger Anwendungen ist daher zeitaufwendig und anfällig für Laufzeitfehler. Hier sollte Adobe in zukünftigen Versionen nachbessern, um sich dem von Java auf der Serverseite längst gewohnten Komfort anzunähern.

Auch die Programmiersprache SSAS ist in die Jahre gekommen: Basierend auf einer alten Version von Actionscript lässt ihr Funktionsumfang zu wünschen übrig. Es fehlen viele wichtige objektorientierte Merkmale, die auf der Client-Seite bereits seit Action-

Listing 2: *Main.hx*

```
import flash.net.NetConnection;
import flash.net.ObjectEncoding;
import flash.events.NetStatusEvent;
import flash.display.Sprite;
import flash.text.TextField;
import flash.text.TextFormat;
class Main {
    static public var root:Sprite;
    public var conn:NetConnection;
    static var output:TextField;
    static function main() {
        root = flash.Lib.current;
        // Textfeld fuer Debug-Ausgabe erzeugen
        output = new TextField();
        output.defaultTextFormat = new TextFormat("verdana", 11);
        output.width = 350;
        output.height = 100;
        output.border = true;
        output.textColor = 0x000000;
        root.addChild(output);
        new Main();
    }
    // Zur Anzeige clientseitiger Debug-Informationen
    public function trace(str) {
        output.text += str + '\n';
    }
    function netstat(stats:NetStatusEvent) {
        if(stats.info.code == "NetConnection.Connect.Success") {
            this.trace("Connection with server established");
        }
        else if(stats.info.code == "NetConnection.Connect.Rejected") {
            this.trace("Connection with server rejected: " +
                  stats.info.application.message);
        }
        else if(stats.info.code == "NetConnection.Connect.Failed") {
            this.trace("Connection with server failed");
        }
    }
    function new() {
        conn = new NetConnection();
        conn.objectEncoding = ObjectEncoding.AMF0;
        conn.addEventListener(NetStatusEvent.NET_STATUS, netstat);
        conn.client = new Client(conn, this);
        try {
            conn.connect("rtmp://localhost/echo");
        }
        catch(ex:Dynamic) {
            trace(ex);
        }
    }
}
```

Die Startklasse der haXe-Client-Anwendung: Eine *NetConnection*-Instanz stellt die Verbindung zum Server her.

Die haXe-Client-Klasse: Deren Methode *say* wird nach erfolgreichem Verbindungsaufbau vom Server aufgerufen.

Listing 3: *Client.hx*

```
import flash.net.NetConnection;
class Client {
    private var _conn:NetConnection;
    private var _main:Main;
    public function new(conn:NetConnection, main:Main) {
        _conn = conn;
        _main = main;
    }
    // Wird vom Server aufgerufen, sobald die Verbindung akzeptiert wurde
    public function setServerTime(timeMessage:String) {
        say("Server time is " + timeMessage);
        // 'echo' auf dem Server aufrufen
        _conn.call("echo", null, "Client is calling echo() on server");
    }
    // 'Wird vom Server aufgerufen, um den Client zu einer Ausgabe zu
    // veranlassen
    public function say(str:String) {
        _main.trace(str);
    }
}
```



In der Administrationskonsole erscheinen die Meldungen des Flash-Servers (Abb. 1).

script 2 (im Folgenden kurz AS2) und insbesondere mit AS3 Einzug gehalten haben [2]. Dies hat zur Folge, dass man bei der Nutzung von Actionscript auf Server- und Client-Seite ständig gedanklich zwischen zwei Welten umschalten muss.

haXe als Alternative zu Actionscript 3

In einem gewissen Rahmen lassen sich auch ohne die kommerzielle Flash-IDE Anwendungen für den Flash Player realisieren. Zwar gibt es für das komfortable Zusammenstellen und Bearbeiten von Grafiken und Animationen auf dem Bildschirm keine freien Alternativen zu Adobes IDE, wohl aber für die Programmierung in Actionscript. So lässt sich AS2 mit dem plattformunabhängigen Kommandozeilen-Compiler MTASC [f], der in die freie Actionscript-Entwicklungsumgebung Flash Develop [g] integrierbar ist, in Flash-Bytecode übersetzen. Gegenüber dem AS2-Compiler bietet MTASC sogar den Vorteil einer strengeren Fehlerprüfung zur Übersetzungszeit, was die Gefahr von Laufzeitfehlern reduziert. MTASC wird allerdings im Hinblick auf neue Versionen von Actionscript nicht mehr weiterentwickelt. Diese Lücke schließt als Nachfolger der Compiler haXe [h]. Eine Integration in Flash Develop ist bei haXe zurzeit nur für die Version 2 möglich, nicht aber für die Betaversionen von Flash Develop 3.

Anders als MTASC, bei dessen Entwicklung man auf Quelltext-Kompatibilität zu Adobes AS2-Compiler Wert gelegt hat, ist haXe kein AS3-Compiler im eigentlichen Sinne. Die gleichnamige Programmiersprache haXe ist zwar eng mit AS3 verwandt, verfolgt aber einen nicht ausschließlich auf die Kodierung in Actionscript zugeschnittenen Ansatz: haXe zielt auch auf die Entwicklung von Webanwendungen in Javascript ab. Per Compiler-Schalter lassen sich haXe-Quelltexte nach AS3 oder Javascript konvertieren, was haXe zu einem interessanten Compiler-Frontend für diese Sprachen macht. Aber auch die direkte Erzeugung von Flash-Bytecode als SWF-Datei erlaubt der Compiler. Da er die Flash-Client-APIs vollständig unterstützt, lassen sich alle Funktionen der Flash Player 8 und 9 ohne Einschränkungen abrufen.

Die Listings 2 und 3 zeigen einen einfachen haXe-Client, der mit der vorgestellten Server-Anwendung kommuniziert. Die Verwandtschaft der haXe-eigenen Sprache mit AS3 oder Java ist offensichtlich, und die verwendeten Klassenbibliotheken stammen aus dem AS3-Fundus. Die Verbindung zum Server erfolgt über eine *NetConnection*-Instanz, die für den Verbindungsaufbau die URL der Server-Anwendung erwartet. Die URL beginnt mit dem Protokollnamen *rtmp* (Real Time Messaging Protocol) oder *rtmpt/rtmps*, falls die Verbindung über HTTP/HTTPS getunnelt werden soll. Es folgen die Namen des Server-Host, der hier dem lo-


Listing 4: *client.html*

```
<html>
<head>
<title>haXE-Client</title>
</head>
<body>
<object type="application/x-shockwave-flash" data="client.swf"
  width="500" height="500" />
</body>
</html>
```

Zur Darstellung im Browser benötigt das Flash-Plug-in einen HTML-Wrapper für die SWF-Datei des Clients.

kalen Host entspricht, und der Anwendung, die im gleichnamigen Verzeichnis unterhalb des Ordners *applications* auf dem Server liegt. Folgende Kommandozeile kompiliert den Quellcode:

```
haxe -swf-version 9 -main Main -swf client.swf ⁊
                                    Client.hx Main.hx
```

Die Ergebnisdatei *client.swf* lässt sich mit dem Flash Player 9 direkt starten. Für Testzwecke ist es vorteilhaft, den Player in der Entwickler-Variante zu verwenden, die SWF-Dateien ohne Zutun eines Webbrowsers ausführt [i]. Bei Verwendung des Browser-Plug-ins wird neben der SWF-Datei ein HTML-Wrapper wie in Listing 4 benötigt.

Nach dem Start der Anwendung meldet der Flash-Server im Logfile beziehungsweise der Administrationskonsole, dass er eine neue Client-Verbindung eingerichtet und die aktuelle Server-Zeit an den Client gesendet hat (Abbildung 1). Gleichzeitig zeigt der Flash Player eine Meldung über den erfolgreichen Verbindungsaufbau und die Zeitinformation an, die er vom Server erhalten hat. Der Aufruf der Server-Methode *echo()* durch den Client sollte ebenfalls protokolliert worden sein. Meldet das Flash-Plug-in stattdessen einen Security-Error, sind die Sicherheitseinstellungen des Player zu restriktiv und erfordern eine Anpassung. Sie lassen sich im Kontext-Menü (rechte Maustaste) einstellen und sind so zu wählen, dass der Zugriff des Player auf die Datei *client.swf* im lokalen Dateisystem-Pfad zugelassen ist.

Aus den in Listing 2 benutzten Klassenbibliotheken geht hervor, dass sich die von Flash/Actionscript bekannten

Onlinequellen

[a] Flash Player	www.adobe.com/products/player_census/flashplayer/
[b] Open Source Flash	www.osflash.org
[c] Flash Media Server	www.adobe.com/products/flashmediaserver/
[d] Wowza Media Server	www.wowzamedia.com
[e] Red5 Open Source Flash Server	www.osflash.org/red5/
[f] AS2-Compiler MTASC	www.mtasc.org
[g] Flash Develop ActionScript-Editor	www.flashdevelop.org
[h] Compiler haXe	www.haxe.org
[i] Stand-alone-Flash-Player	www.adobe.com/support/flashplayer/downloads.html

Klassen und grafischen Komponenten auch mit haXe programmatisch erzeugen und ansprechen lassen. Dazu unterstützt haXe zwei Flash-Bibliotheken, von denen die eine kompatibel zu Flash 8 (AS2, Flash Player 8 und 9) und die andere kompatibel zu Flash CS3 (AS3, Flash Player 9) ist.

Das rein programmatische Zusammenstellen von Komponenten für eine grafikzentrierte Flash-Anwendung bereitete allerdings wenig Freude. Selbst weitere freie Werkzeuge wie *swfmill*, die auf den Open-Source-Flash-Webseiten gelistet werden [b], und mit denen sich SWF-Dateien mit grafischen Komponenten zusammenstellen und manipulieren lassen, stellen keine wesentliche Erleichterung dar. Hier ist die Flash-IDE den quelloffenen Anwendungen, die sich in erster Linie mit Aspekten der Programmierung und kaum des Oberflächen-Designs beschäftigen, eindeutig überlegen. Es bietet sich aber immerhin eine Arbeitsteilung an, bei der das grafische Design innerhalb der IDE und die Erstellung der Anwendungslogik anschließend ganz oder teilweise mit haXe erfolgt, sei es nativ oder mit anschließender Konvertierung der Quelltexte nach Actionscript 3.

Fazit

Mit Flash lassen sich zusammen mit geeigneten Servern auch Webanwendungen aus dem Client/Server-Bereich entwickeln. Neben den bekannten kommerziellen Tools gibt es dazu eine Reihe freier Werkzeuge aus dem Flash/Actionscript-Umfeld, wobei diese allerdings nicht optimal aufeinander abgestimmt sind.

Zur Erzeugung grafikintensiver Anwendungen eignet sich freie Software kaum, da eine der Flash-IDE vergleichbare freie Entwicklungsumgebung nicht vorhanden ist. Im Bereich der Anwendungslogik hingegen lassen sich kostenlose Werkzeuge für die Client-Seite durchaus produktiv einsetzen, wie die Compiler MTASC und haXe zeigen. Voraussetzung ist, dass der Entwickler die vielbeschworene Trennung von Programmlogik und grafischer Oberfläche konsequent beachtet.

haXe-basierte Anwendungen eignen sich auch für die Realisierung clientseitiger Unit-Tests, insbesondere zur Überprüfung der Logik einer Server-Anwendung. Wer sowohl Applikationen für Javascript als auch für Actionscript entwickelt, profitiert zudem von der Möglichkeit, haXe-kompatible Quelltexte nicht nur direkt in SWF-Dateien übersetzen, sondern die Quellen auch nach Actionscript oder Javascript konvertieren zu können. (ka)

DR. UWE SEIMET

leitet die Abteilung IT/Software beim Cinetic Internet Systemhaus, Karlsruhe.

Literatur

[1] Brian Lesser; Programming Flash Communication Server; O'Reilly 2005

[2] Kai König; Scripting in Action; Professionelle Webanwendungen mit Actionscript 3; *iX* 7/07, S. 66





Prozessorunabhängig optimierte Funktionen

Rechnen wie geölt



Michael Riepe

Kommt es auf maximale Rechenleistung an, muss der Programmierer die besonderen Eigenschaften des Prozessors ausnutzen. Leider sind die so entstandenen Programme nicht mehr portabel. Die Bibliothek *liboil* kann Abhilfe schaffen.

Nicht alle Rechner sind gleich. Ein Lied davon können die Nutzer von Supercomputern singen: Einen guten Teil ihrer Zeit verbringen sie damit, ihre Software für den vorhandenen Rechner zu optimieren. Wechseln sie irgendwann auf ein anderes Modell, geht die Arbeit von vorn los.

Ähnlich geht es den Entwicklern von Multimedia-Anwendungen oder Audio- und Video-Codecs. Programmiert man allein in der Hochsprache, läuft die Software zu langsam. Nutzt man die Besonderheiten der Prozessorarchitektur – etwa MMX/SSE-Befehle bei AMD- und Intel-CPUs oder die Altivec-Einheit beim PowerPC –, ist sie hingegen nicht länger portabel.

Sowohl bei wissenschaftlichen als auch bei Multimedia-Anwendungen verbringt die CPU viel Zeit in Programmschleifen. Daher lohnt es sich, die in die Schleife eingebetteten Anweisungen zu untersuchen und gegebenenfalls zu optimieren – oder durch vorgefertigte, optimierte Routinen zu ersetzen.

Eine Sammlung solcher Routinen bietet die Library of Optimized Inner Loops *liboil* (siehe Kasten „Onlinequellen“) von David Schleef, dem Entwickler des Dirac-Video-Codecs *Schrödinger*. Sie kommt sowohl dort als auch im Multimedia-Framework *gstreamer* zum Einsatz und bietet aktuell gut 400 Funktionen für das Rechnen mit Vektoren und Matrizen.

Für jede Funktion gibt es eine Referenzimplementierung, die den Maßstab für Geschwindigkeit und Genauigkeit setzt. Daneben kann es mehrere optimierte Varianten geben. Beim ersten Aufruf wählt *liboil* automatisch die schnellste. Versionen, die falsch rechnen oder unbekannte Befehle verwenden, schließt die Bibliothek jedoch aus.

Vor dem ersten Funktionsaufruf muss das Programm mit *oil_init();* die Bibliothek initialisieren. Die Namen der übrigen Funktionen folgen dem Schema *oil_<funktion>_<argumenttypen>*: *oil_conv_f64_s32* etwa rechnet 32-Bit-Integer vom Typ *int32_t* in 64-Bit-Gleitkommazahlen (*double*) um. Die entgegengesetzte Operation heißt *oil_clipconv_s32_f64*. Sie rundet gebrochene Zahlen zur nächstliegenden ganzen Zahl; ob *0.5* auf- oder abgerundet wird, hängt von der jeweiligen Implementierung ab. Der Zusatz *clip* im Funktionsnamen deutet an, dass sich bei der Konversion nicht alle Werte auf den neuen Typ abbilden lassen und die Funktion daher gegebenenfalls den Wertebereich begrenzen (clippen) muss.

Onlinequellen

liboil
liboil.freedesktop.org/wiki/

liboil Manual
liboil.freedesktop.org/documentation/

Dirac und Schrödinger
www.diracvideo.org

gstreamer
gstreamer.freedesktop.org

Listing 1: oil_conv_f64_s32

```
void oil_conv_f64_s32(
     /* Zielvektor und Schrittweite */
     double *dest,
     int dstr,
     /* Quellvektor und Schrittweite */
     const int32_t *src,
     int sstr,
     /* Zahl der zu berechnenden Elemente */
     int n)
{
     while (n > 0) {
          *dest = round((double)*src);
          dest += dstr;
          src += sstr;
          --n;
     }
}
```

Durch die variablen Schrittweiten lassen sich Funktionen wie *oil_conv_f64_s32* universell einsetzen.

Single Instruction, Multiple Data

Als Argumente erwarten die Funktionen in der Regel Vektoren – in C also Zeiger auf das erste Element des Vektors. Mitunter muss man für jeden Vektor eine Schrittweite („stride“) angeben, außerdem die Zahl der zu berechnenden Elemente. *oil_conv_f64_s32* etwa benötigt fünf Argumente (siehe Listing 1).

Mit *oil_permute_<typ>* lassen sich die Elemente eines Vektors neu anordnen. Spezialfälle wie das bei der MPEG-Video-Kompression vorkommende Transponieren 8 × 8 Elemente großer Makroblöcke oder die „Zickzack“-Konvertierung erledigen *oil_trans 8x8_<typ>*, *oil_zigzag8x8_<typ>* und *oil_unzigzag8x8_<typ>*.

Daneben beherrscht *liboil* die gängigen (Vektor-)Operationen mit jeweils mehreren Datentypen. Zusätzlich zu den elementweise durchgeführten Grundoperationen lassen sich das Skalarprodukt, die Summe der Elemente und der Betrag eines Vektors berechnen, Konstanten zu den Elementen addieren oder Vektoren mit Skalaren multiplizieren.

Außerdem gibt es eine Reihe von Operationen für MPEG-Makroblöcke wie Matrix-Multiplikation, die Berechnung des Unterschieds zweier Blöcke oder die Diskrete Cosinus-Transformation (DCT, IDCT). Daneben existieren optimierte Funktionen für die Pixel-Manipulation und das Konvertieren zwischen verschiedenen Farbdarstellungen wie ARGB und AYUV.

Definitionsgemäß ist *liboil* ein Projekt, das niemals fertig wird. Kommen neue Prozessoren auf den Markt, ergeben sich neue Gelegenheiten, den Code zu optimieren. Außerdem lassen sich jederzeit neue nützliche Funktionen hinzufügen. Hier sind vor allem die Anwendungsentwickler aufgerufen, ihren Teil beizusteuern. (mr)

iX-Link ix0806142





Cross-Site Request Forgery verhindern

Mein Cookie gehört mir

Tina Müller

Cookies gibt es überall im Web: Sie speichern Einstellungen oder authentifizieren Benutzer. Das ist bequem und vermeidet Session-IDs in der URL, birgt aber auch Gefahren.

Wer beim Besuch eines Onlineshops ein Produkt im eigenen Warenkorb entdeckt, ohne es jemals auch nur angesehen zu haben, ist möglicherweise Opfer einer Attacke, die Cookies ausnutzt. In diesem Fall bietet der Shop dem Nutzer ein langfristig gültiges Cookie, damit er sich für Warenkorb-Aktionen nicht extra anmelden muss. Erst beim Kaufvorgang verlangt die Website das Passwort. Das ist zwar grundsätzlich eine gute Idee, birgt jedoch Risiken bei unzureichendem Schutz seitens des Servers, da Browser das Cookie bei Warenkorb-Aktionen automatisch mitsenden und im Formular nur benutzerunabhängige Felder liefern müssen.

Einen Angriff, der das ausnutzt, nennt man Cross-Site Request Forgery (CSRF, „Onlinequellen“ [a]). Zunächst soll ein kleines Beispiel zeigen, was genau passiert. Darauf aufbauend folgen mögliche Lösungswege sowie Gründe, die gegen andere Lösungen sprechen.

Als Mini-Beispiel fungieren hier statt des Warenkorbs ein Forum und die Funktion des Artikelschreibens. Es ist auf alle Anwendungen übertragbar, die sich nur auf Cookies verlassen. Der Nutzer ist mit einer eine Stunde gültigen Session-ID (SID) auf der Site A (www.forum.example) angemeldet. Diese SID steht in einem Cookie, das der Browser bei jedem Request an Site A im HTTP-Header mitsendet.

Das Formular zum Artikelschreiben enthalte ein Textfeld, einen Knopf zum Abschicken und ein verstecktes Feld mit der Aktion, die das serverseitige Programm ausführen soll. Der Browser schickt somit an die Seite www.forum.example/script:

```
article=Lorem Ipsum
submit_article=Abschicken
action=post_article
```

sowie die SID im Cookie.

Angriffe von vielen Seiten

Ein Angreifer hat mehrere Möglichkeiten, dieses Formular zu versenden, ohne dass der Nutzer das möchte. Webseite B (www.fremd.example), auf die der Nutzer etwa durch eine Suchmaschine gelangt ist, kann ein *img*-Element das *src*-Attribut

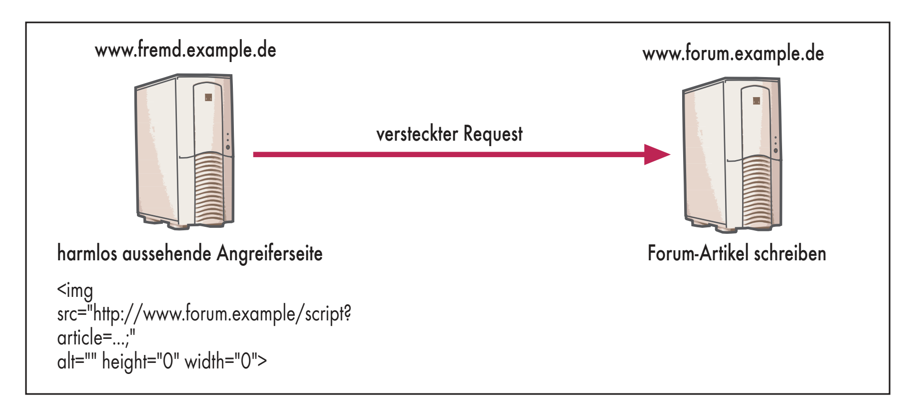
```
http://www.forum.example/script? \
  article=...;submit_article=Abschicken;\
  action=post_article
```

enthalten (s. Abb. 1). Statt eines Bildes funktionieren auch Javascript- und CSS-Dateien, Iframes, Redirect und Meta-Refresh. Ohne Zutun des Nutzers und unbemerkt von ihm schickt der Browser in allen diesen Fällen das Formular ab.

Prüft Webseite A, ob das Formular per *POST* eintrifft, verhindert dies den Angriff, da die genannten Links nur einen *GET*-Request auslösen. Es gibt jedoch noch andere Möglichkeiten. Auf der Webseite B kann sich ein vorausgefülltes, verstecktes Formular befinden, das ein Submit-Button abschickt, ohne dass der Benutzer sich dessen bewusst ist. Bei aktiviertem Javascript hat man leichtes Spiel, so kann die Seite ein Formular automatisch abschicken.

In keinem der genannten Fälle gelangt das Cookie an die fremde Site B, was den Angriff von klassischem XSS (Cross-Site Scripting) unterscheidet, jedoch sendet der Browser das Cookie vertrauensvoll an A. So kann man also mit einer manipulierten Webseite Forums-Artikel unter dem Namen anderer veröffentlichen oder Produkte in anderer Leute Warenkörbe legen.

Da es ein passiver Angriff ist, muss man warten, bis ein mögliches Opfer auf die manipulierte Webseite kommt. Bei



Ein verstecktes Bild löst einen Request auf eine andere Domain aus.

vielbesuchten, populären Webseiten kann es sich lohnen, Nutzer durch gute Suchmaschinenplatzierung auf die Seite zu locken. Bei einer kleineren Nutzergemeinde hilft unter Umständen das gezielte Verschicken von Links auf diese Seite.

Leichtes Spiel mit dem Router

CSRF ist weniger bekannt als XSS oder SQL-Injections und noch selten im Einsatz, gewinnt jedoch mittlerweile an Aufmerksamkeit. Beispiele sind Angriffe auf lokale Router. Viele von ihnen sind standardmäßig unter derselben lokalen IP-Adresse zu erreichen (192.168.0.1), und mit CSRF kann man so die Router-Einstellungen ahnungsloser Nutzer verändern, wenn diese gerade eingeloggt sind [b]. Verstärkt tritt dieser Angriff auf, wenn die Router-Software statt Cookies nur Basic-Authentication verwendet, da solche Sessions in der Regel bis zum Beenden des Browsers bestehen. Einige Browser bieten allerdings die Möglichkeit, sich durch manuelles Löschen der Anmeldedaten „auszuloggen“. Auch bekannte Content-Management-Systeme haben es mit solchen Lücken schon in die News geschafft [c].

Keine einfache Lösung im Browser

Weitgehenden Schutz böte eine Einstellung, mit der „eingebettete“ Anfragen von Domain B auf Domain A keine Cookies liefern. In Opera gibt es schon lange die Option „Nur Cookies der besuchten Seite annehmen“, die in einem Test mit Opera 9.5 Beta das Gewünschte erledigte. Für Firefox existiert die Extension Cookiesafe und die Einstellung *originalOnly*, die jedoch im Test nicht zuverlässig funktionierte. Was bei beiden Angeboten fehlt, ist eine ausführliche Dokumentation, bei welchen Requests diese Einstellung genau zum Tragen kommt. Des Weiteren sind solche Umsetzungen anfällig, da es sehr viele CSRF-Attacken gibt, die sie alle erkennen müssen. Die Möglichkeiten von Javascript erschweren diese Aufgabe zusätzlich.

Zudem würde diese Einstellung gewünschte Effekte verhindern. Externe Seitenzähler, die viele Firmen anbieten, funktionierten nicht mehr richtig. Authentifizierungsmechanismen wie OpenID würden behindert, da hier ein Redirect auf den OpenID-Anbieter stattfindet, der kein Cookie mehr erhielte. Ein Test mit Opera unter dieser Einstellung verhinderte das Einloggen mit OpenID bis die weiterleitende Domain manuell freigegeben war.

Diskussionen auch mit Webentwicklern zeigen, dass zum einen bisher relativ wenig Wissen zu diesem Thema vorhanden ist und zum anderen oft nicht auf Anhieb der Unterschied zu XSS verstanden wird. Deshalb existieren viele unterschiedliche Meinungen darüber, wie sich Browser verhalten sollten. Solange es also keine verlässliche Einstellung in allen Browsern gibt, muss man serverseitig ansetzen.

Das Feld *Referer* im HTTP-Header scheint genau die gewünschte Funktion zu besitzen; es enthält im Normalfall die URL, von der der aktuelle Request ausging. Als Programmierer müsste man es nur prüfen und auf einige wenige Ausnahmen achten. Beispielsweise könnte eine Forums-Seite einen Artikel mit einem manipulierten Link und gleichzeitig das „echte“ Formular beinhalten, der Referer wäre also fälschlicherweise korrekt. Hier muss man bei allen Links, die aus Nutzereingaben stammen können, einen Zwischen-Redirect schalten. Auch manipulierbar ist der Referer in diesem Fall nicht, da sich der Browser unter Nutzerkontrolle befindet. Fälschen lässt er sich nur, wenn man selbst etwa mit einem Skript einen Request absetzt.

Doppelt hält nicht immer besser

Jedoch gibt es Proxies, die keinen oder veränderte Referer schicken; außerdem kann man bei den meisten Browsern die Übermittlung des Referer abschalten, um die Privatsphäre zu schützen. Würde er jedoch immer korrekt übertragen, wäre seine Prüfung die Lösung der Wahl.

Die einfachste von einigen Forumssystemen eingesetzte Möglichkeit ist, die SID sowohl im Cookie wie in einem versteckten Feld des Formulars abzulegen. Damit ist man auf der sicheren Seite, und für viele kleine Anwendungen reicht das aus. Allerdings hat dieses Vorgehen zwei Nachteile. Zum einen steht die SID im Quelltext und ist somit leichter ausspähbar; etwa indem ein Nutzer eine solche Seite speichert und verschickt. Technischen Laien ist schwer zu vermitteln, warum das gefährlich sein kann. Zum anderen büßt man so den Komfort eines permanenten Cookie ein. Viele Seiten bieten über die SID hinaus ein solches Cookie, damit sie Kunden am eigenen PC immer automatisch erkennen. Kommen sie etwa nach zwei Stunden auf die Forumsseite zurück, ist zwar die SID abgelaufen, aber dank des permanenten Cookie erstellt der Server automatisch eine neue. Ein noch geöffnetes Formular enthält jedoch die alte SID, sodass der Server es nicht akzeptiert. An dieser Stelle bräuchte man eine zwischengeschaltete Bestätigungsseite.

Um beiden Nachteilen zu entgehen, benötigt man eine zweite SID, zum Unterscheiden hier „Token“ genannt, das wesentlich länger gelten kann als die SID. Die Anwendung generiert eines pro Nutzer und speichert es in der Datenbank. Alle Formulare enthalten seinen Wert in einem versteckten Feld. Der Angreifer kann somit kein gültiges Formular vorausfüllen, da er das Token nicht kennt. Mit dieser Änderung schickt der Browser beim Absenden des Beispielformulars Folgendes an www.forum.example/script:

```
article=Lorem Ipsum
submit_article=Abschicken
action=post_article
token=1234567890abcdef...
```

sowie die SID im Cookie. Versendet ein Nutzer so ein Formular per Mail, kann man zwar das Token auslesen, jedoch damit alleine nichts anfangen. Die SID ist unabhängig vom Token und gerät so nicht in fremde Hände.

Das Token kann man genau wie eine klassische SID implementieren, sodass der Server das Ablaufdatum bei jedem Klick neu setzt; die einzigen Unterschiede sind die längere Gültigkeitsdauer und der Übertragungsweg Formular statt Cookie. Der Programmierer muss nur sicherstellen, dass es tatsächlich nach einer bestimmten Zeit abläuft, denn ein ewig gültiges Token wäre zu riskant.

Bei diesem Verfahren besteht nur noch die Gefahr einer gezielten Attacke auf eine Person. Späht ein Angreifer auf irgendeinem Weg das Token aus, kann er genau diesen Nutzer auf eine manipulierte Seite locken. Um auch solche Angriffe zu verhindern, kann man Tokens implementieren, die jeweils einem Nutzer und einer Aktion zugeordnet sind. In der Datenbank stünde dann:

user_id	action	token	expire
42	post_article	1234abcd...	2008-04-17 15:00:00

Das Abschicken des Formulars löscht das Token sofort. Dieses Vorgehen erfordert etwas mehr Programmieraufwand, bietet aber größere Sicherheit, da ein Token nur noch für eine bestimmte Aktion gilt.

Fazit

CSRF ist noch relativ unbekannt, und Angriffe sind passiv. Lücken auszunutzen, erfordert gründliches Testen der Webanwendung oder genaue Kenntnis des Quellcodes. Jedoch können Angreifer Lücken ohne Bemerken des Nutzers ausnutzen, was je nach Anwendung zu unangenehmen Konsequenzen führt, wenn etwa empfindliche Daten oder Geld im Spiel sind. Browserseitig können sich bisher allenfalls erfahrene Nutzer etwas schützen, weshalb hier die Webentwickler in der Pflicht stehen, ihre Seiten beziehungsweise ihre Nutzer zu schützen. (ck)

Onlinequellen

[a] Cross-Site Request Forgery	de.wikipedia.org/wiki/CSRF
[b] Angriff auf Router	www.heise.de/security/Praeparierte-Webseite-schaltet-Firewall-im-Router-aus--/news/meldung/101641
[c] Angriff auf CMS	www.heise.de/security/Sicherheitsluecken-in-WordPress--/news/meldung/83280

TINA MÜLLER

arbeitet bei der imt GmbH in Berlin und ist seit mehreren Jahren als Entwicklerin von Backends für Webseiten tätig. Ihre Programmiersprache der Wahl ist Perl.





Mineralwasser als Lebensspender

Eingetaucht

Diane Sieger

Ob Kaffee-, Cola- oder Weintrinker – eins haben sie gemeinsam: Ohne einen ordentlichen Schluck Leitungs- oder Mineralwasser täglich geht es nicht.

Der menschliche Körper besteht zu einem großen Teil aus Wasser; im Erwachsenenalter zu etwa 60 Prozent, bei Säuglingen beträgt der Anteil sogar bis zu 75 Prozent (www.inform24.de/wasser.html). Da der Mensch ununterbrochen Flüssigkeit über Atemluft, Harn oder Schweiß ausscheidet, muss eine ständige Versorgung von außen gewährleistet sein. Am einfachsten geht das durch Trinken von Mineralwasser. Ein guter Grund, das Thema Wasser einmal genauer zu betrachten.

Hierzulande ist es nicht sonderlich schwierig, an Informationen über Mineralwasser zu gelangen, denn Deutschland ist ein Mineralwasserland. Über 500 Sorten in unterschiedlichen Zusammensetzungen gelangen von den deutschen Mineralbrunnen in den Handel – nachzulesen bei der Informationszentrale Deutsches Mineralwasser (IDM) unter www.mineralwasser.com/fakten/fakten/index.php. Laut IDM ist diese Vielfalt weltweit einzigartig, die Webseite „Mineral Waters of the World“ listet jedoch unter www.mineralwaters.org für Italien noch einige Wässer mehr auf als für Deutschland. Auf dieser Non-Profit-Webseite finden sich über 3000 unterschiedliche Marken aus 125 Ländern, inklusive einer Auflistung ihrer Inhaltsstoffe und der Möglichkeit, Wassermarken zu bewerten. Ein Verbraucherportal rund ums Wasser, dessen Design zwar ein wenig zu wünschen übrig lässt, das inhaltlich jedoch einen Blick wert ist.

Wasser ist nicht gleich Wasser. In Deutschland wird zwischen Heil-, Mineral-, Quell-, Tafel- und Trinkwasser unterschieden. Die gesetzlich festgesetzten Definitionen regeln die zulässigen Verfahren für Gewinnung, Herstellung und Kennzeichnung sowie zulässige Inhaltsstoffe. Wer es genauer wissen möchte, sollte sich die Seminararbeit von Daniela Heinrich (www.goek.tu-freiberg.de/oberseminar/OS_05_06/daniela_heinrich.pdf) aus dem Oberseminar Geoökologie aus dem Jahre 2006 zu diesem Thema durchlesen. Natürlich ist die offizielle Verordnung über natürliches Mineral-, Quell- und Tafelwasser auch als Gesetzestext beim Bundesministerium der Justiz unter www.gesetze-im-internet.de/min_tafelwv abrufbar.

Wasser ist kein Lebensmittel

Erstaunlicherweise zählt in Flaschen verpacktes Wasser in Deutschland offiziell nicht als Lebensmittel. Zumindest steuerrechtlich muss der Verkäufer den 19%igen Mehrwertsteuersatz aufschlagen, nicht nur den sonst bei Lebensmitteln üblichen 7%igen ermässigten Steuersatz. Einen Auszug aus der Liste der dem ermässigten Steuersatz unterliegenden Gegenstände gibt es beim Shopblogger (www.shopblogger.de/blog/archives/6183-19%25-auf-Wasser.html).

Früher war die Beschaffung von Trinkwasser recht beschwerlich. Man musste mit Eimern zum nächstgelegenen See oder Fluss pilgern und das kühle Nass von dort nach Hause tragen (www.was-wir-essen.de/abisz/gewinnung_gesundes_trinkwasser.php) oder Wasserlöcher anlegen, aus denen mithilfe von Schildkrötenpanzern oder Birkenrinde das Wasser abgeschöpft werden konnte (de.wikipedia.org/wiki/Brunnen).

Dagegen ist das Wassertrinken heute kinderleicht. Es gibt im Wesentlichen zwei Methoden. Erstens: den Wasserhahn öffnen und das Wasser frisch in das Glas laufen lassen, gegebenenfalls filtern oder mit Kohlensäure versetzen. Zweitens: in den Supermarkt spazieren und die Wasserflasche der Wahl in den Einkaufswagen legen.

Bleibt die Frage, woher das Wasser heute eigentlich kommt. Wie das kühle Nass über das mehr als 400 000 Kilometer lange Wasserleitungssystem in Deutschland bis in den häuslichen Wasserhahn gelangt, erklärt der Westdeutsche Rundfunk im Internetangebot zu seiner Sendung „Quarks & Co“ unter www.wdr.de/tv/quarks/sendungsbeitraege/2005/0712/04_wasser_zu_trinkwasser.jsp. Den Weg vom Brunnen in die Flasche hingegen erläutert das in Kooperation mit dem Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz entstandene Webangebot von was-wir-essen.de anschaulich unter www.was-wir-essen.de/abisz/wasser_verarbeitung_aufbereitung.php.

Die Mär vom Krieg der Flaschen

Als der durchschnittliche *iX*-Leser noch ein Kind war, kam das Mineralwasser typischerweise in klassischer 0,7-Liter-Glasflasche mit vertrautem Perlendekor, an der man sich bei ersten Versuchen, das Aus-der-Flasche-Trinken zu erlernen, fast die Zähne ausschlagen konnte. Heutzutage gewinnt die PET-Flasche zunehmend an Popularität. Die Vorteile der Plastikverpackung liegen klar auf der Hand: Durch das geringere Gewicht der Flaschen sind selbst Füllmengen von bis zu 1,5 oder 2 Litern für den Verbraucher noch einfach zu handhaben. Auch der durch Coca Cola in den frühen 90ern geprägte Begriff „unkaputtbar“ (de.wiktionary.org/wiki/unkaputtbar) spiegelt einen enormen Vorteil der PET-Flasche wider: Sie ist nahezu unzerstörbar. Doch PET hat auch Gegner, die sich massiv gegen eine Ausbreitung der Plastikflasche wehren. Hauptkritikpunkt: Durch das geringe Gewicht und günstig gestaltete Kästen brauchen die Brunnen weniger Lkw-Fuhren mit geringerem Benzinverbrauch, um das Wasser im Land zu verteilen. Dies zerstöre die mittelständische Erzeugerstruktur, da regionale Abfüllanlagen weniger gebraucht würden. Detailliert nachzulesen im Zeit-Artikel „Krieg der Flaschen“ unter www.zeit.de/1995/13/Krieg_der_Flaschen?page=1.

Doch nicht nur die Flasche steht im Fadenkreuz der Kritiker, oftmals gibt es um das Wasser direkt oder seine Herstellungsmethoden einen Aufschrei. Beispielsweise als Hersteller Adelholzener für sein ActiveO2 Wasser im Jahre 2003 auf Tierversuche setzte. Um die bis

dahin wenig erforschte und durchaus umstrittene Wirkung des mit Sauerstoff angereicherten Wassers zu belegen, führte Adelholzener Tests an Kaninchen durch und befand sich bald im Fadenkreuz einer groß angelegten Kampagne engagierter Tierschützer. Aufgrund des enormen Protestes stellte er die Tierversuchsreihe glücklicherweise ein – nachzulesen ist diese Erfolgsgeschichte beim Tierschutzbund unter www.tierschutzbund.de/00366.html.

Bislang ging es hier vornehmlich um die positiven Aspekte des Trinkwassergenusses. Allerdings ist der Genuss von Wasser nicht immer frei von Gefahren. Verbraucherschutzorganisationen schlagen nach Mineralwassertests regelmäßig Alarm. Ob Uran im kohlensäurehaltigen Wasser (www.youtube.com/watch?v=t2Nhch79gxQ) oder Krankheitskeime im stillen Wasser (www.youtube.com/watch?v=9Q_Wfth9Hsw&feature=related), für Menschen mit Abwehrschwächen kann durch den Genuss verunreinigten Wassers sogar eine lebensbedrohliche Situation entstehen.

Doch trotz regelmässiger Schreckensmeldungen: Wasser ist und bleibt eines der wichtigsten Grundnahrungsmittel. Der Mensch kann zwar ohne Essen bis zu 30 Tage überleben, hält es ohne Wasseraufnahme aber nur zwei bis vier Tage aus (www.lifeline.de/special/getraenke_trinken/mineralwasser/content-128727.html). Deshalb sollte man die drohende Weltwasserkrise nicht aus den Augen verlieren. Bereits heute leben 1,1 Milliarden Menschen ohne Zugriff auf sauberes Trinkwasser, und wenn man den Ausführungen des World Water Councils (worldwatercouncil.org/index.php?id=25) folgt, lassen sich weitere drastische Einschränkungen erwarten. Kein Wunder, ist doch ein Großteil des Weltwasservorkommens für die Ernährung von Menschen vollkommen ungeeignet (www.intaqua.de/wasserglobus). (ka)

URLs auf einen Blick

www.inform24.de/wasser.html
www.mineralwasser.com/fakten/fakten/index.php
www.mineralwaters.org
www.goek.tu-freiberg.de/oberseminar/OS_05_06/daniela_heinrich.pdf
www.gesetze-im-internet.de/min_tafelwv
www.shopblogger.de/blog/archives/6183-19%25-auf-Wasser.html
www.was-wir-essen.de/abisz/gewinnung_gesundes_trinkwasser.php
de.wikipedia.org/wiki/Brunnen
www.wdr.de/tv/quarks/sendungsbeitraege/2005/0712/04_wasser_zu_trinkwasser.jsp
www.was-wir-essen.de/abisz/wasser_verarbeitung_aufbereitung.php
de.wiktionary.org/wiki/unkaputtbar
www.zeit.de/1995/13/Krieg_der_Flaschen?page=1
www.tierschutzbund.de/00366.html
www.youtube.com/watch?v=t2Nhch79gxQ
www.youtube.com/watch?v=9Q_Wfth9Hsw&feature=related
www.lifeline.de/special/getraenke_trinken/mineralwasser/content-128727.html
worldwatercouncil.org/index.php?id=25
www.intaqua.de/wasserglobus

Wer weitere URLs zum Thema kennt, hat die Möglichkeit, sie der Online-Version (www.heise.de/ix/artikel/2008/06/146/) hinzuzufügen.

Vor 10 Jahren: Lizenz zum Burgenbauen

Auf den ersten Blick haben Programmierer und Juristen wenig gemeinsam. Doch bei näherem Hinsehen schlüpfen viele Softwareentwickler auch immer wieder ganz gerne in den Talar des Advokaten mit mehr oder weniger weltanschaulichem Impetus.

Das „Lizenzcenter“ des Instituts für Rechtsfragen der Freien und Open Source Software führt etwa 200 verschiedene Lizenzen für quelloffene Software und ihre Dokumentationen auf. Eine *iX* zu diesem Thema könnte es locker auf eine Doppelnummer bringen. Matthias Kalle Dalheimer, vielen Lesern als Entwickler des grafischen Benutzerinterfaces KDE bekannt, macht dafür eine heimliche Leidenschaft verantwortlich, die Programmierer und Juristen gemeinsam haben: „So wie jeder Programmierer irgendwann im Leben einen eigenen Mail-Client schreibt, muss wohl jeder Open-Source-Advokat irgendwann seine eigene Lizenz schreiben.“

Vor 10 Jahren sah die Lizenzwelt kaum übersichtlicher aus, als *iX* in Ausgabe 6/98 mit mehreren Artikeln einen „Wegweiser im Lizenzdschungel“ aufstellte. Ausführlich wurde die X11-Lizenzpolitik besprochen, komplett mit Stellungnahmen des konkurrierenden XFree86 Project und der Open Group. Unter dem leicht frivolen Titel „Sandkastenspiele“ bemühte sich Matthias Dalheimer, die wichtigsten Lizenzen der BSD-, GPL- und LGPL-Familien vorzustellen. Anders als es der Titel vielleicht suggeriert, behandelte Dalheimer die einzelnen Lizenzprojekte nicht als Kampf um das richtige Förmchen und die korrekte Schaufel, sondern schilderte die jeweiligen Vorteile und Nachteile für konkrete Entwicklungsprojekte.

Von einer journalistischen Darstellung abweichend, erklärte Dalheimer damals die Sicht des Entwicklers. „Im Gegensatz zu einigen Hardlinern bin ich nicht der Meinung, dass jede kommerzielle Software ein Werk des Teufels ist. Beide haben ihre Berechtigung, und sei es nur, um den Entwicklern einen vollen Kühlschrank zu sichern. Als freischaffender Softwareentwickler spüre ich die Ambivalenz zwischen freien und kommerziellen Anwendungen täglich am eigenen Leibe – und zwar im positiven Sinne. Durch die Entwicklung kommerzieller Applikationen kann ich meine Familie ernähren und habe gleichzeitig die Möglichkeit, freie Software zu schreiben.“

Von diesem entspannten Ansatz gegenüber den unterschiedlichen offenen wie kommerziellen Lizenzmodellen ist Dalheimer auch nach 10 Jahren überzeugt. „Meine Haltung hat sich in der Angelegenheit nicht verändert, ich verwende grundsätzlich die für eine Aufgabe am besten geeignete Software, egal ob kommerziell oder nicht. In der Welt, in der ich mich bewege, ist freie Software aber oft überlegen oder die einzige Alternative.“ In seiner auf dreißig Mitarbeiter angewachsenen Firma hat Dalheimer zwar das Programmieren aufgegeben, nicht aber die Prinzipien. Aber einen Mail-Client könnte er noch schreiben und unter die erweiterte kleine Dalheimer-Lizenz stellen. Jederzeit. *Detlef Borchers*

MEHR KBYTES

Softwareentwicklung

Agil heißt so viel wie beweglich, tätig, gut. Kein Wunder, dass der Begriff es in die Softwareentwicklung geschafft hat. Dass agile Programmierung nicht einfach Rumwuseln bedeutet, lehren Kent Beck und viele andere seit Jahren. Ob XP oder Scrum, agil zu programmieren will gelernt sein. Dies zu unterstützen, vor allem was XP angeht, haben James Shore und Shane Warden „The Art of Agile Development“ geschrieben, das O’Reilly im vorigen Herbst veröffentlicht hat – anders als die Nutshell-Bände ohne Tier auf dem Cover; stattdessen zenartiges Gewächs im Glas. Die Anspielung auf eine potenziell lange Lehrzeit unterstreicht das Serienmotto „Theory/in/Practice“.

Die Autoren führen zunächst ins Thema ein, um anschließend die Eigenheiten des Extreme Programming darzustellen. Im dritten Teil schließlich beschäftigen sie sich damit, wie man XP an die eigenen Bedürfnisse anpasst. Dass nicht einmal Agiles der Königsweg der Softwareentwicklung sein kann – oder gar eine Wunderwaffe im Kampf gegen scheiternde Projekte (Brooks’ „silver bullet“) –, heben Shore und Waren hervor.

Beim ersten Blick auf Wolf-Gideon Bleeks und Henning Wolfs „Agile Softwareentwicklung“ liegt wegen der bunten Ballons der Gedanke an Smalltalk-80 nahe. Die beiden Autoren haben mit ihrem Band jedoch bei dpunkt soeben eine Einführung ins Agile veröffentlicht, die außer XP Scrum und Feature Driven Development (FDD) einbezieht. An den Komponenten Management, Team und Entwicklung orientiert, stellen sie Fragen, deren Beantwortung aus den unterschiedlichen Methoden stammen kann.

Über verspätet ausgelieferte oder gescheiterte Projekte klagen viele. Leistungseinbrüche im Betrieb sind zwar seltener Gegenstand der Diskussion, beanspruchen aber insbesondere im Zeitalter netzweiter Software und serviceorientierter Architektur (SOA) mehr Aufmerksamkeit. Christof Schmalenbachs bei Springer in der Reihe Xpert.press erschienenes „Performancemanagement für serviceorientierte Java-Anwendungen“ will hier helfen. Der Autor beschreibt zunächst Rollen und Aufgaben von IT-Architekten, Entwicklern und anderen und diskutiert die Zusammensetzung des Performanceteams. Anschließend geht es um quantitative Methoden, später um Kapazitätsplanung und die Simulation von Geschäftsprozessen. Nicht zu vergessen Java-Überwachung und die Leistungsfähigkeit von Webservices. Administratoren, Projektverantwortliche wie Entwickler sollten sich angesprochen fühlen.



Trotz Websprachen wie PHP dürfte das Entweder-oder in der Anwendungsprogrammierung, vor allem bei den sogenannten Rich Clients, .Net oder Java sein. Als Werkzeuge kommen Visual Studio oder Eclipse infrage, was nichts gegen andere heißt.

Berthold Daums Eclipse-Buch liegt mittlerweile in der dritten, überarbeiteten Auflage vor. „Rich-Client-Entwicklung mit Eclipse 3.3“, wiederum bei dpunkt erschienen, stellt dar, wie Programmierer die dafür notwendigen Plug-ins erzeugen können. Bei RCP kein Wunder: GUI-Fragen nehmen mit SWT und JFace einen großen Umfang ein. Darüber hinaus behandelt Daum Persistenzfragen (XML, RDBMS) und das Eclipsesche Graphical Editing Framework (GEF). Kein Buch für Einsteiger; Leser sollten etwas mit generischen Typen anfangen können.

Auf der anderen Seite nennen Rainer Stropek und Karin Huber Rich Clients lieber Full Clients. Ihr „WPF und XAML Programmierhandbuch“, das die entwickler.press gerade veröffentlicht hat, behandelt die Arbeit mit der Windows Presentation Foundation und vor allem der „neuen“ XML Application Markup Language (XAML), die für WPF und die Windows Workflow Foundation (WF) von Bedeutung ist. Ob Data Binding, 2D, Animation oder 3D, Benutzerschnittstellenexperten der Windows-Forms-Ära haben viel zu lesen.

Wer den Internet Explorer verstoßen und sich beispielsweise Firefox zugewandt hat, kann, entsprechende Fähigkeiten vorausgesetzt, Rich Clients mit Mozillas XML User Interface Language entwickeln. Jonathan Protzenkos XUL-Buch ist bei der Open Source Press in deutscher Übersetzung erschienen und zeigt, was man mit der Sprache anstellen kann: Durchgängiges Projekt des Buches ist eine Forensoftware. Nichts für IE-Fans, stattdessen für Mozilla-affine Entwickler gedacht.

Wer Rich Client sagt, denkt wohl auch an Adobes Flash – beziehungsweise Flex oder AIR. O’Reilly hat Chafic Kazouns und Joey Lotts „Programmieren mit Flex 2“ auf Deutsch veröffentlicht. Wie der Verlag mitteilt, lässt das Buch sich für die Arbeit mit der Version 3 ebenfalls nutzen. Die Autoren führen in MXML und Actionscript ein und widmen sich Layoutcontainern, unterschiedlichen Medien, Datenkommunikation und Fehlersuche. Weitere Bücher zu Flex 3 sollen im Sommer auf den Markt kommen.

Henning Behme

Wolf-Gideon Bleek, Henning Wolf; Agile Softwareentwicklung; Werte, Konzepte, Methoden; Heidelberg (dpunkt) 2008; 187 Seiten; € 29,– (Paperback)

Berthold Daum; Rich-Client-Entwicklung mit Eclipse 3.3; Anwendungen entwickeln mit Eclipse RCP, SWT, Forms, GEF, BIRT, JPA u. a. m.; Heidelberg (dpunkt) 2008; 3., überarbeitete und erweiterte Auflage; 640 Seiten; € 49,– (gebunden)

Chafic Kazoun, Joey Lott; Programmieren mit Flex 2; übersetzt von Sascha Kersken und Peter Klicman; Köln (O’Reilly) 2008; 523 Seiten; € 54,90 (gebunden)

Jonathan Protzenko; XUL; Entwicklung von Rich Clients mit der Mozilla XML User Interface Language; München (Open Source Press) 2007; übersetzt von Dinu Gherman; 351 Seiten; € 39,90 (gebunden)

Christof Schmalenbach; Performance-Management; für serviceorientierte Java-Anwendungen; Berlin, Heidelberg (Springer) 2007; 267 Seiten; € 49,95 (Paperback)

James Shore, Shane Warden; The Art of Agile Development; Sebastopol, CA (O’Reilly Media) 2007; 409 Seiten; € 38,– (Paperback)

Rainer Stropek, Karin Huber; WPF und XAML; Programmierhandbuch; Frankfurt/Main (entwickler.press) 2008; 593 Seiten zzgl. CD-ROM; € 49,90 (gebunden)



Werner Eberling, Jan Leßner

Enterprise JavaBeans 3

München, Wien 2007
Carl Hanser
290 Seiten
39,90 €
ISBN 978-3-446-41085-5

Keine Programmiersprache weckt so lebendige Assoziationen mit Konzepten wie Wiederverwendbarkeit, Komponentenarchitektur und Application Server wie Java. Java Beans sind wiederverwendbare Komponenten, die auf der Client-Seite genutzt werden, während man mit dem EJB-Standard Komponenten auf der Server-Seite implementiert. Dazu bedarf es eines Application Server, der den Beans eine Reihe wichtiger Funktionen fertig anbietet.

Werner Eberlings und Jan Leßners Buch hilft, auf die neue Version 3 des Standards zu migrieren. Wie andere Hanser-Bücher ist es praxisorientiert, nach einer kurzen Einführung erklären die Autoren die Grundbegriffe, die für das weitere Verständnis des Buches wichtig sind: Schichtenarchitektur, Komponenten sowie das JDK und die Java Enterprise Edition. Schon im zweiten Kapitel wird eine Entwicklungsumgebung installiert.

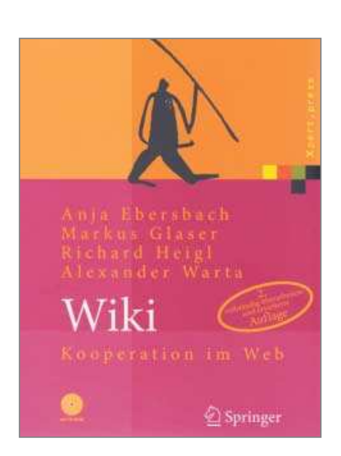
Nach der erfolgreichen Implementierung der ersten Bean stellen die Autoren Sessions Beans vor. Dabei gehen sie wie in den folgenden Kapiteln auf Unterschiede der Standards 2.0 und 3.0 ein. Im anschließenden Kapitel widmen sie Entities mit 80 Seiten den Löwenanteil des Buches. Hier lernt man alles über Persistenz, objektrelationales Mapping und Zugriff auf Objekte mittels Datenbankabfragen.

Nach einem Kapitel über Messaging (inklusive Java Messaging Service, JMS) gehen die Autoren genauer auf die Konfiguration einer EJB ein. Danach folgt ein Kapitel, das einen wichtigen Aspekt in der Programmierung von Anwendungen darstellt: Transaktionen. Persistenz, Container und per Bean verwaltete Transaktionen, Rollforward und Rollback werden hier genauer erklärt.

Authentifizierung und Verschlüsselung stehen im Zentrum des Kapitels über Sicherheit. Es folgt eins, das Aspektorientierung in EJBs, Timed Objects und Object Handles als Alternative zu Remote References beschreibt. Außerdem eins, das sich mit dem Testen von EJBs, Patterns und der Migration zu EJB 3 beschäftigt.

Wer sich in die Welt der EJBs einarbeiten will, ist mit diesem Buch gut bedient. Es bietet reichlich Code, der auf der Webseite zum Download zur Verfügung steht. Im Preis ist die elektronische Version des Buches inbegriffen.

REINHARD VOGLMAIER



Anja Ebersbach, Markus Glaser, Richard Heigl, Alexander Warta

Wiki

Kooperation im Web

Berlin, Heidelberg 2007
Springer Verlag
2., vollständig überarbeitete und erweiterte Auflage
529 Seiten
39,95 €
ISBN 978-3-5403-5110-8

Nach E-Mail, FAQ, Instant Messaging und Open-Source-Software wandern nun Wiki-Systeme vom Internet ins Intranet großer wie kleiner Unternehmen. Im Gegensatz zu den im Enterprise gewohnten sperrigen „Knowledge Management Systemen“ kosten Wikis praktisch gar nichts, schaffen eine egalitäre, transparente Plattform für flache Hierarchien und sind enorm flexibel und praktisch.

Die erste Frage, die sich vor der Einführung eines Wikis stellt: Welches System verwenden? Hingegen ist die erste Frage, die sich immer stellen sollte: Kann die eigene Organisation so viel Transparenz und Egalität verkraften?

Solche und andere Fragen erörtert „Wiki – Kooperation im Web“, in der ersten Auflage schon 2005 erschienen und Ende letzten Jahres völlig überarbeitet, von Springer veröffentlicht. Die vier Autor(inn)en sind Berater und haben ein Kompendium geschrieben, das den aktuellen Wissenstand zur Technik, Philosophie und Praxis von Wikis gut zusammenfasst. Das Buch vergleicht drei Systeme und beleuchtet deren Stärken, Schwächen, Merkmale, Installation und Betrieb, um zukünftigen Wiki-Mastern eine technische Grundlage für ihre Entscheidung zu liefern. Die technischen Fragen sind im Betrieb aber nicht die allein wichtigen, daher kommt die Erörterung firmenpolitischer und sozialer Punkte ebenfalls nicht zu kurz.

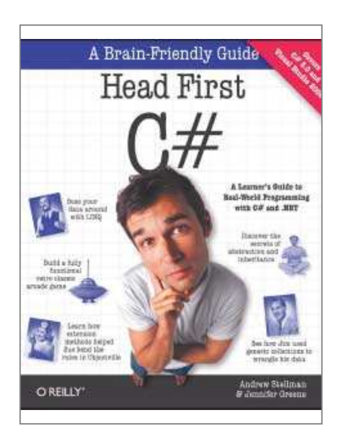
Wikis sind nützlich, erfordern aber flankierende organisatorische und operative Maßnahmen; einfach nur ein System auf einem Server zu installieren ist zu wenig. Wikis als soziale Software haben wegen ihres emanzipatorischen Charakters durchaus subversive Aspekte. Dass nach der Einführung niemand etwas schreibt, gehört noch zu den harmloseren Pleiten, die passieren können.

Aus diesem Grund sehen viele die Wiki-Technik unter dem Blickwinkel möglicher Irritationen für Mitarbeiter und Vorgesetzte. Das Werk ist durchsetzt von einleuchtenden (oft witzigen) Beispielen, Szenarien, Anekdoten und Motiven.

Die Autoren liefern eine detaillierte Einführung zu drei Systemen: dem in PHP geschriebenen MediaWiki (Open Source, das System hinter Wikipedia), dem in Perl entwickelten TWiki (Open Source) sowie dem in Java geschriebenen Confluence der australischen Firma Atlassian (inklusive kommerzieller Lizenzen).

Unter anderem erläutern die Autoren Fragen und Empfehlungen wie die titelgebende Kollaboration im Wiki, Moderatoren für Projekte und Teams, Konflikte, Vandalismus und mehr. Der Autor dieser Rezension wurde übrigens erst nach einer gründlich missglückten Wiki-Einführung auf den Band aufmerksam. Bedauerlich, denn Anfängerfehler zu vermeiden wäre nicht schwierig gewesen, wie das Buch demonstriert.

REINHARD GANTAR



Andrew Stellman, Jennifer Greene

Head First C#

Sebastopol, CA 2007
O'Reilly Media
778 Seiten
48,– €
ISBN 978-0-596-51482-2

Die Vorgehensweise der mittlerweile etablierten Head-First-Reihe von O'Reilly setzt einen aktiven Leser voraus, der sich nicht davor scheut, „ein paar Neuronen zu strapazieren“. Auf die zahlreichen Geschichten in zwangloser Sprache, visuellen Reize und anderen Kniffe, die Aufmerksamkeit des Lesers zu erregen – und den Übergang des Stoffes vom Kurzzeit- in das Langzeitgedächtnis zu unterstützen – muss sich der Leser einlassen.

Andrew Stellmans und Jennifer Greenes „Head First C#“ behandelt die Programmiersprache in Version 3.0 sowie Visual Studio 2008. Kapitel 1 eröffnet mit Entwurf und Umsetzung einer Kontaktverwaltung. Hier lernt der Leser schnell, wie er mit Visual Studio 2008 eine Benutzerschnittstelle (mit Windows.Forms) gestaltet und ein Datenbankschema entwirft sowie die zugehörigen Tabellen anlegt. Unter Verwendung der nötigen .Net-Komponenten ist die gewünschte Kontaktverwaltung schnell umgesetzt. Das folgende „Under the Hood“ verdeutlicht, dass der Entwickler nicht nur ein IDE-Benutzer ist, sondern darüber hinaus die zugrunde liegende Programmiersprache beherrschen muss. An dieser Stelle wird eine Einführung in die Syntax von C# gegeben, bevor Stellman und Greene die darauf aufbauenden Konzepte der objektorientierten Programmierung behandeln.

„Storing lots of data“ widmet sich „enums“ und „collections“, Kapitel 9 zeigt unter anderem, wie File I/O in .Net beziehungsweise mit C# funktioniert. Unter der Überschrift „Putting out fires gets old“ erklären Autor und Autorin das Konzept der Behandlung von Fehlern mit Exceptions. Die für die GUI-Programmierung wichtigen Konzepte Events und Delegates sind ein weiteres Thema. Das zwölfte Kapitel nimmt eine Sonderstellung ein, da es Themen der vorangegangenen vertieft sowie einen Ausblick auf die folgenden gibt, in denen es unter anderem um Grafikprogrammierung und LINQ geht.

Gegenüber anderen Büchern aus der Reihe zeichnet sich „Head First C#“ durch die ausführlichen, gelungenen und „verspielten“ Beispielprojekte aus, bei denen der Leser sein Wissen bei der Programmierung klassischer Spielkonzepte wie rundenbasiertem Rollenspiel in die Praxis umsetzt.

SEBASTIAN BERGMANN



MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

Postfach 61 04 07, 30604 Hannover; Helstorfer Straße 7, 30625 Hannover

Redaktion
Telefon: 05 11/53 52-387, Fax: 05 11/53 52-361, E-Mail: post@ix.de
Abonnements: Telefon: 0711/72 52-292, Fax: 0711/72 52-392, E-Mail: abo@heise.de

Herausgeber: Christian Heise, Ansgar Heise

Redaktion: Chefredakteur: Jürgen Seeger (JS) -386

Stellv. Chefredakteur: Henning Behme (hb) -374

Ltd. Redakt.: Kersten Auel (ka) -367, Ralph Hülsenbusch (rh) -373, Bert Ungerer (un) -368

Jürgen Diercks (jd) -379, Christian Kirsch (ck) -590, Wolfgang Möhle (WM) -384, Susanne Nolte (sun) -689, André von Raison (avr) -377, Michael Riepe (mr) -787, Ute Roos (ur) -535

Redaktionsassistenz: Carmen Lehmann (cle) -387, Michael Mentzel (mm) -153

Korrespondent Köln/Düsseldorf/Ruhrgebiet:
Achim Born, Siebengebirgsallee 82, 50939 Köln,Telefon: 02 21/4 20 02 62,
E-Mail: ab@ix.de

Korrespondentin München:
Susanne Franke, Ansbacherstr. 2, 80796 München, Telefon: 089/28 80 74 80,
E-Mail: sf@ix.de

Ständige Mitarbeiter: Torsten Beyer, Detlef Borchers, Fred Hantelmann, Kai König, Michael Kuschke, Barbara Lange, Stefan Mintert, Holger Schwichtenberg, Susanne Schwonbeck, Christian Segor, Diane Sieger, Axel Wilzopolski, Nikolai Zotow

DTP-Produktion: Enrico Eisert, Wiebke Preuß, Matthias Timm, Hinstorff Verlag, Rostock

Korrektorat/Chefin vom Dienst: Anja Fischer

Fotografie: Martin Klauss Fotografie, Despetal/Barfelde

Titelidee: ***iX;*** Titel- und Aufmachergestaltung: Dietmar Jokisch

Verlag und Anzeigenverwaltung:
Heise Zeitschriften Verlag GmbH & Co. KG, Postfach 61 04 07, 30604 Hannover;
Helstorfer Straße 7, 30625 Hannover; Telefon: 05 11/53 52-0, Fax: 05 11/53 52-129

Geschäftsführer: Ansgar Heise, Steven P. Steinkraus, Dr. Alfons Schräder

Mitglied der Geschäftsleitung: Beate Gerold

Verlagsleiter: Dr. Alfons Schräder

Anzeigenleitung: Michael Hanke -167, E-Mail: michael.hanke@heise.de

Assistenz: Christine Richter -534, E-Mail: christine.richter@heise.de

Anzeigendisposition: Christine Richter -534, E-Mail: christine.richter@heise.de

Anzeigenverkauf: PLZ-Gebiete 0–3, Ausland:
Oliver Kühn -395, E-Mail: oliver.kuehn@heise.de,
PLZ-Gebiete 8–9: Ralf Räuber -218, E-Mail: ralf.raeuber@heise.de
Sonderprojekte: Isabelle Paeseler -205, E-Mail: isabelle.paeseler@heise.de

Anzeigen-Inlandsvertretung: PLZ-Gebiete 4–7:
Karl-Heinz Kremer GmbH, Sonnenstraße 2, D-66957 Hilst,
Telefon: 063 35/92 17-0, Fax: 063 35/92 17-22, E-Mail: karlheinz.kremer@heise.de

Anzeigen-Auslandsvertretung:
Großbritannien, Irland: Oliver Smith & Partners Ltd. Colin Smith, 18 Abbeville Mews, 88 Clapham Park Road, London SW4 7BX, UK, Telefon: (00 44) 20/79 78-14 40, Fax: (00 44) 20/79 78-15 50,
E-Mail: colin@osp-uk.com

Anzeigenpreise: Es gilt die Anzeigenpreisliste Nr. 20 vom 1. Januar 2008.

Leiter Vertrieb und Marketing: Mark A. Cano (-299)

Werbeleitung: Julia Conrades (-156)

Teamleitung Herstellung: Bianca Nagel (-456)

Druck: Dierichs Druck + Media GmbH & Co. KG, Kassel

Sonderdruck-Service: Bianca Nagel (-456, Fax: -360)

Verantwortlich: Textteil: Jürgen Seeger; Anzeigenteil: Michael Hanke

iX **erscheint monatlich**

Einzelpreis € 5,50, Österreich € 6,20, Schweiz CHF 10,70, Benelux € 6,70, Italien € 6,70

Das Abonnement für 12 Ausgaben kostet: Inland € 56,–, Ausland (außer Schweiz) € 63,–; Studentenabonnement: Inland € 42,–, Ausland (außer Schweiz) € 47,– nur gegen Vorlage der Studienbescheinigung (inkl. Versandkosten Inland € 8,30, Ausland € 13,30), Luftpost auf Anfrage.

iX-Abo+ (inkl. jährlicher Archiv-CD-ROM) jeweils zzgl. € 8,–

Für GI-, VDI-KfIT-, GUUG-, IUG-, LUG-, AUGE- und Mac-e.V.-Mitglieder gilt der Preis des Studentenabonnements (gegen Mitgliedsausweis).

Kundenkonto in Österreich:
Dresdner Bank AG, BLZ 19675, Kto.-Nr. 2001-226-00 EUR, SWIFT: DRES AT WX

Kundenkonto in der Schweiz: UBS AG, Zürich, Kto.-Nr. 206 P0-465.060.0

Abo-Service:
Heise Zeitschriften Verlag, Kundenservice, Postfach 810520, 70522 Stuttgart,
Telefon: 0711/72 52-292, Fax: 0711/72 52-392, E-Mail: abo@heise.de

Für Abonnenten in der Schweiz Bestellung über:
Thali AG, Aboservice, Industriestr. 14, CH-6285 Hitzkirch,
Telefon: 041/919 66 11, Fax: 041/919 66 77, E-Mail: abo@thali.ch, Internet: www.thali.ch (Jahresabonnement: CHF 111,–; Studentenabonnement: CHF 83,25)

Das Abonnement ohne Archiv-CD-ROM ist jederzeit mit Wirkung zur jeweils übernächsten Ausgabe kündbar. Das *iX-Abo+* (incl. jährlicher Archiv-CD-ROM) gilt zunächst für ein Jahr und ist danach zur jeweils übernächsten Ausgabe kündbar.

Vertrieb Einzelverkauf (auch für Österreich, Luxemburg und Schweiz): MZV Moderner Zeitschriften Vertrieb GmbH & Co. KG, Breslauer Str. 5, 85386 Eching, Telefon: 089/319 06-0, Fax: 089/319 06-113, E-Mail: mzv@mzv.de, Internet: www.mzv.de



ISSN 0935-9680



Backup mit freien Tools

Ob eine Backup-Lösung etwas taugt oder nicht, hängt von einem garantiert nicht ab: dem Preis. Viel wichtiger ist das Know-how der Administratoren, ihre Erfahrungen, was womit gut zusammenspielt. Ein Erfahrungsbericht zum Thema Netzwerk-Backup anhand des freien Tool-Sets Bacula.

Kreditkartenanbieter fordern IT-Sicherheit

Seit Jahren doktert die Kreditwirtschaft an verbindlichen Sicherheitsmaßnahmen für Kreditkarten-Transaktionen herum. Der neueste Vorschlag ist der Payment Card Industry Data Security Standard (PCI DSS), auf dessen praktische Umsetzung die Kreditkartenanbieter jetzt drängen. Mittlerweile hagelt es sogar schon Vertragsstrafen bei Unterlassungssünden.

Eclipse-Alternative: Netbeans 6

Der Siegeszug der Java-Entwicklungsplattform Eclipse scheint nicht enden zu wollen. Im Windschatten davon hat sich aber auch Netbeans in den letzten Jahren gut weiterentwickelt und bietet inzwischen eine ernstzunehmende Alternative zu Eclipse. Netbeans verfügt über einen Profiler und GUI-Designer, mit denen sich schnell entwickeln lässt. Wirklich große Neuerungen hat die Version 6 zwar nicht zu bieten, sie überzeugt aber in den Details.

Heft 07/2008 erscheint am 19. Juni 2008

Herstellerübergreifende RDBMS-Verwaltung

In kaum einem Unternehmen läuft nur das Datenbanksystem eines Herstellers. In der Regel sind zwei oder mehr unterschiedliche Produkte in Betrieb, die jeweils ihre eigenen Verwaltungswerkzeuge mitbringen. Herstellerübergreifende Werkzeuge bieten eine einheitliche Oberfläche für unterschiedliche RDBMSe an und vereinfachen die Arbeit. *iX* stellt die Produkte in einer Marktübersicht vor.



Bilddateien in Java laden

Von Haus aus unterstützt Java nur wenige Bildformate, in die ein Bild konvertiert werden muss, wenn man es in eine Java-Anwendung lädt. Wer das nicht will – etwa weil die Abbildung für die Archivierung im Originalzustand erhalten bleiben soll – kann sich mit dem ImageIO Framework behelfen. Mit dessen Hilfe lässt sich leicht ein Service-Provider programmieren, der die Verarbeitung neuer Formate gestattet.